Number Theory and Algebra

EDITED BY

HANS ZASSENHAUS

Number Theory and Algebra

ZASSENHAUS

512.
7
NUM

ACADEMIC PRESS

ADVISORY BOARD OF THE JOURNAL OF NUMBER THEORY

RANKO BOJANIC

ROBERT GOLD

JOHN HSIA

MANOHAR MADAN

ALAN WOODS

Number Theory and Algebra

Collected Papers Dedicated to Henry B. Mann, Arnold E. Ross, and Olga Taussky-Todd

Edited by
HANS ZASSENHAUS
DEPARTMENT OF MATHEMATICS
THE OHIO STATE UNIVERSITY
COLUMBUS, OHIO

with the collaboration of the Advisory Board
of the Journal of Number Theory

ACADEMIC PRESS New York San Francisco London 1977
A Subsidiary of Harcourt Brace Jovanovich, Publishers

ACCESSION No. 119011

CLASS No. 512.7 NUM

22 NOV 1978

N CATEGORY

COPYRIGHT © 1977, BY ACADEMIC PRESS, INC.
ALL RIGHTS RESERVED.
NO PART OF THIS PUBLICATION MAY BE REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC OR MECHANICAL, INCLUDING PHOTOCOPY, RECORDING, OR ANY INFORMATION STORAGE AND RETRIEVAL SYSTEM, WITHOUT PERMISSION IN WRITING FROM THE PUBLISHER.

ACADEMIC PRESS, INC.
111 Fifth Avenue, New York, New York 10003

United Kingdom Edition published by
ACADEMIC PRESS, INC. (LONDON) LTD.
24/28 Oval Road, London NW1

Library of Congress Cataloging in Publication Data

Main entry under title:

Number theory and algebra.

Includes bibliographical references.
1. Numbers, Theory of–Addresses, essays, lectures. 2. Algebra–Addresses, essays, lectures. 3. Mann, Henry Berthold. 4. Ross, Arnold Ephraim, Date 5. Taussky, Olga. I. Zassenhaus, Hans. II. Mann, Henry Berthold. III. Ross, Arnold Ephraim, Date IV. Taussky, Olga.
QA241.N866 512'.7 77-9365
ISBN 0-12-776350-3

PRINTED IN THE UNITED STATES OF AMERICA

Contents

List of Contributors xiii

Preface xvii

Biographical Sketches xix

Henry B. Mann xxi
Arnold E. Ross xxvii
Olga Taussky-Todd xxxv

Octaves and Modular Forms **1**

BRAM VAN ASCH

Introduction 1
References 5

On the Product of Three Inhomogeneous Linear Forms **7**

R. P. BAMBAH AND A. C. WOODS

1. Introduction 7
2. The Main Lemmas 8
3. Proof of the Theorem 9
4. Proof of Lemma 1 10
5. Proof of Lemma 2 11

References 17

On the Degrees of the Sum and Product of Two Algebraic Elements **19**

BOHUSLAV DIVIŠ

References 27

Indices in Cyclic Cubic Fields 29

D. S. DUMMIT AND H. KISILEVSKY

References 42

Spinor Genera under Field Extensions, III: Quadratic Extensions 43

A. G. EARNEST AND J. S. HSIA

1. Computation of $\mathrm{Ker}(\psi_L)$ 45
2. Spinor Norms in Quadratic Fields 51
3. Applications 59

References 62

On Products of Consecutive Integers 63

P. ERDÖS AND E. G. STRAUSS

1. Introduction 63
2. The Case $k \geq \delta n$ 66
3. The Case $A(m, k) \equiv 0 (\mathrm{mod}\ A(n, k))$; $n + k \leq m \leq \Delta n$ and $\{n + 1, \ldots, n + k\}$ Contains a Prime 69
4. Open Questions 70

Non-Abelian Jacobi Sums 71

A. FRÖHLICH

Introduction 71
1. Statement of Results 72
2. The Evaluation Pairing 73
3. Resolvents 74

References 75

The Hasse Norm Theorem for l-Extensions of the Rationals 77

DENNIS A. GARBANATI

Introduction 77
1. Preliminaries 78
2. A Criterion for the Hasse Norm Theorem to Hold 81
3. The Structure of $(G, G)/(G, H)$ for Fields with Properties (I)–(IV) 81
4. The Hasse Norm Theorem for Fields with Properties (I)–(IV) 86

References 90

Scalar Extensions of Binary Lattices 91

ROBERT GOLD AND PAUL PONOMAREV

References 95

Quartic Coverings of a Cubic 97

BASIL GORDON AND MURRAY SCHACHER

Introduction 97
1. Groups Admissible over All Number Fields 98
2. Covering a Resolvent Cubic 99
References 101

On Extremal Density Theorems for Linear Forms 103

R. L. GRAHAM, H. S. WITSENHAUSEN, AND J. H. SPENCER

1. Introduction 104
2. Preliminaries 104
3. Augmented Arithmetic Progressions 104
4. Forms in One Variable—A Special Case 106
5. Forms in One Variable—The General Case 108
6. Concluding Remarks 109
References 109

Aliquot Sequences 111

RICHARD K. GUY

References 117

Integral Matrices A for which $AA^{\mathrm{T}} = mI$ 119

MARSHALL HALL, JR.

1. Introduction 119
2. Existence Conditions 120
3. Rational Completions and Orthogonal Equivalence 122
4. Results on Integral Completions 124
5. Integral Completions for Hadamard Matrices 127
References 134

Lie Algebraic Proofs of Some Theorems on Partitions 135

J. W. B. HUGHES

1. Introduction 135
2. $A(n-1)$ 138

3. $B(n)$ 145
4. $C(n)$ 150
5. $D(n)$ 153
References 155

On Prime Numbers $\equiv$ 1 resp. 3 mod 4 **157**

S. KNAPOWSKI AND P. TURÁN

References 165

Signatures on Frobenius Extensions **167**

MANFRED KNEBUSCH

Introduction 167
1. The Transfer Formula 169
2. Some Examples 174
3. Integral Extensions of Semilocal Rings 178
4. Frobenius Extensions with One Generator 183
References 186

Generalizations of Gauss's Lemma **187**

EMMA LEHMER

References 194

On $|\alpha|^2 + |\beta|^2 = p^l$ in Certain Cyclotomic Fields **195**

SUNDER LAL, R. L. MCFARLAND, AND R. W. K. ODONI

Galois Cohomology and a Theorem of E. Artin **199**

MANOHAR L. MADAN AND SAT PAL

1. Introduction 199
2. Galois Cohomology 200
3. A Theorem of E. Artin 206
References 208

On Some Special Decimal Fractions **209**

K. MAHLER

References 214

Sums from a Sequence of Group Elements 215

JOHN E. OLSON AND EDWARD T. WHITE

1. Introduction 215
2. Notation and Preliminaries 216
3. Proof of the Theorem 217
References 222

Concerning a Possible "Thue–Siegel–Roth Theorem" for Algebraic Differential Equations 223

CHARLES F. OSGOOD

Introduction 223
References 234

The Minimum Discriminant of Seventh Degree Totally Real Algebraic Number Fields 235

M. POHST

References 240

On Absolutely Irreducible Representations of Orders 241

WILHELM PLESKEN

Introduction 241
References 262

The Existence of *P*-adic Abelian *L*-functions 263

CARY QUEEN

Introduction 263
1. Preliminaries 264
2. *p*-adic Modular Quasiforms 268
3. Modular Forms on $\Gamma_{0\,1}(p^r, N)$ 271
4. *p*-adic *L*-functions 282
References 287

A Characterization of the Line–Hyperplane Design of a Projective Space and Some Extremal Theorems for Matroid Designs **289**

D. K. RAY-CHAUDHURI AND N. M. SINGHI

1. Introduction 289
2. Preliminaries 293
3. Proof of Theorem 1 294
4. Geometric Designs 298
References 301

On the Behavior of Ideal Classes in Cyclic Unramified Extensions of Prime Degree **303**

ROSS SCHIPPER

1. Introduction 303
2. Proof of Theorem 3 305
3. Construction of K_1 and K_2 306
References 309

Irregularities of Distribution, X **311**

WOLFGANG M. SCHMIDT

1. Introduction 311
2. The Method 313
3. Generalized Rademacher Functions 314
4. Estimation of Moments 316
5. Construction of an Auxiliary Function 318
6. Proof of Theorem 1 319
7. Proof of Theorem 2 319
8. Estimation of Sums 320
9. Preparations for Theorem 3 323
10. A Lemma 325
11. Proof of Theorem 3 328
References 328

Prime Ideal Decomposition in $F(\mu^{1/m})$, II **331**

WILLIAM YSLAS VÉLEZ

1. Introduction 331
2. Theorems and Proofs 332
References 338

Rational Quadratic Forms and Orthogonal Designs 339

WARREN WOLFE

References 348

On Finite Projective Planes of Lenz–Barlotti Class I3 349

JILL C. D. S. YAQUB

References 361

A Theorem on Cyclic Algebras 363

HANS ZASSENHAUS

Introduction 363
1. Simple Properties of Cyclic Algebras 364
2. A Theorem on Cyclic Algebras 366
3. The Spectral Decomposition Belonging to Maximal Commutative Subalgebras 368
4. Crossed Product Rings 373
5. Crossed Product Orders 384
6. Valuation Theoretic Interpretation 391

References 393

List of Contributors

Numbers in parentheses indicate the pages on which the authors' contributions begin.

R. P. BAMBAH (7), Panjab University, Chandigarh, India
BOHUSLAV DIVIŠ* (19), The Ohio State University, Columbus, Ohio
D. S. DUMMIT (29), Princeton University, Princeton, New Jersey
A. G. EARNEST† (43), Department of Mathematics, The Ohio State University, Columbus, Ohio
P. ERDÖS (63), Hungarian Academy of Science, Budapest, Hungary
A. FRÖHLICH (71), King's College, University of London, London, England
DENNIS A. GARBANATI (77), University of Maryland, College Park, Maryland
ROBERT GOLD (91), Department of Mathematics, The Ohio State University, Columbus, Ohio
BASIL GORDON (97), University of California, Los Angeles, California
R. L. GRAHAM (103), Bell Laboratories, Murray Hill, New Jersey
RICHARD K. GUY (111), University of Calgary, Calgary, Alberta, Canada
MARSHALL HALL, JR. (119), California Institute of Technology, Pasadena, California
J. S. HSIA (43), Department of Mathematics, The Ohio State University, Columbus, Ohio
J. W. B. HUGHES (135), Queen Mary College, London, England
K. KISILEVSKY (29), California Institute of Technology, Pasadena, California
S. KNAPOWSKI* (157), University of Miami, Miami, Florida

* Deceased.

† Present address: Department of Mathematics, University of Southern California, Los Angeles, California.

MANFRED KNEBUSCH (167), Universitaet Regensburg, Regensburg, West Germany
SUNDER LAL (195), Panjab University, Chandigarh, India
EMMA LEHMER (187), Berkeley, California
MANOHAR L. MADAN (199), Department of Mathematics, The Ohio State University, Columbus, Ohio
K. MAHLER (209), Research School of Physical Sciences, Australian National University, Canberra, Australia
R. L. MCFARLAND (195), Wright State University, Dayton, Ohio
R. W. K. ODONI (195), University of Exeter, Exeter, England
JOHN E. OLSON (xxi, 215), The Pennsylvania State University, University Park, Pennsylvania
CHARLES F. OSGOOD (223), Naval Research Laboratory, Washington, D.C.
SAT PAL (199), The Ohio State University, Columbus, Ohio
WILHELM PLESKEN (241), Lehrstuhl D für Mathematik, Technische Hochschulle Aachen, Aachen, West Germany
M. POHST (235), Universität Köln, Cologne, West Germany
PAUL PONOMAREV (91), The Ohio State University, Columbus, Ohio
CARY QUEEN* (263), University of California, Berkeley, California
D. K. RAY-CHAUDHURI (289), Department of Mathematics, The Ohio State University, Columbus, Ohio
MURRAY SCHACHER (97), Department of Mathematics, University of California, Los Angeles, California
ROSS SCHIPPER† (303), Department of Defense, Washington, D.C.
WOLFGANG M. SCHMIDT (311), University of Colorado, Boulder, Colorado, and Universität Wien, Vienna, Austria
N. M. SINGHI (289), The Ohio State University, Columbus, Ohio
J. H. SPENCER‡ (103), Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts
E. G. STRAUS (63), Department of Mathematics, University of California, Los Angeles, California
OLGA TAUSSKY-TODD (xxxv), California Institute of Technology, Pasadena, California
P. TURÁN§ (157), Hungarian Academy of Science, Budapest, Hungary
BRAM VAN ASCH (1), Department of Mathematics, Rijksuniversiteit Utrecht, Utrecht, The Netherlands

* Present address: Department of Mathematics, Cornell University, Ithaca, New York.
† Present address: 6300 Golden Hook, Columbia, Maryland 21044.
‡ Present address: Department of Mathematics, SUNY at Stony Brook, New York.
§ Deceased.

WILLIAM YSLAS VÉLEZ (331), University of Arizona, Tucson, Arizona, and Sandia Laboratories, Albuquerque, New Mexico
EDWARD T. WHITE (215), The Pennsylvania State University, University Park, Pennsylvania
H. S. WITSENHAUSEN (103), Bell Laboratories, Murray Hill, New Jersey
WARREN WOLFE* (339), Queens University, Kingston, Ontario, Canada
A. C. WOODS (7), The Ohio State University, Columbus, Ohio
JILL C. D. S. YAQUB (349), The Ohio State University, Columbus, Ohio
HANS ZASSENHAUS (xxvii, 363), Department of Mathematics, The Ohio State University, Columbus, Ohio

* Present address: Department of Mathematics, Royal Roads Military College, Victoria, British Columbia, Canada.

Preface

We are happy to honor three well-known number theorists, Henry B. Mann, Arnold E. Ross, and Olga Taussky-Todd. We do this at a time when they can look back over many years of honest toil and productive work.

We, their colleagues, pupils, collaborators, and friends find it fitting to dedicate to them the fruits of our work so as to pass on to researchers coming after us the spirit of patient toil in the service of the queenly science which our three honorees implanted in us.

We would like to thank the publisher for encouraging the publication of this special volume. We are also grateful for the overwhelming response by the authors upon this happy occasion.

As a study of the table of contents of this book will suggest to the reader, there is an enormous variety and depth to the research efforts of the modern number theorist and algebraist. As a first guide to the reader who is familiar with the traditional classification of the fields under consideration, we would like to group the contents along the following lines.

Elementary number theory is one of the most ancient sources of number theoretical and algebraic speculation which only now seems to be able to find its true depth. See for example the contribution of "Erdös" type by P. Erdös and E. G. Strauss. Richard K. Guy's contribution has a more experimental flavor. Emma Lehmer follows in the steps of C. F. Gauss (1777–1855). An application of Lie algebra is made by J. W. B. Hughes.

Numbers as objects of *statistical analytic number theory* investigations are dealt with by K. Mahler, by R. L. Graham, H. S. Witsenhausen, and J. H. Spencer; also by Wolfgang M. Schmidt as well as by the late S. Knapowski and P. Turán.

An application of the *theory of modular forms* is given by Bram van Asch.

The *combinatorial aspects of number theory* and their connection with *group theory* are dealt with in the contribution by John E. Olson and Edward T. White; also by Sundar Lal, R. L. McFarland, and R. W. K. Odoni

in response to a challenging problem of H. Mann on difference sets. The *combinatorial properties of finite fields* are dealt with by D. K. Ray-Chaudhuri and N. M. Singhi. An application of such ideas in *finite projective geometry* was made by Jill C. D. S. Yaqub.

The *algebraic theory of quadratic forms and their applications* is expounded by Warren Wolfe. A novel more abstract treatment of the theory is given by Manfred Knebusch.

The classical *arithmetical theory of quadratic forms* is dealt with in the articles by A. G. Earnest and J. S. Hsia, Robert Gold and Paul Ponomarev, and by Marshall Hall, Jr.

The *algebra of finite extensions* was enriched by the late Bohuslav Diviš in reply to a challenging question of A. Schinzl.

The *theory of algebraic number fields and their arithmetics* is richly represented by the contributions of D. S. Dummit and H. Kisilevsky, A. Fröhlich, Dennis A. Garbanati, Basil Gordon and Murray Schacher, Gary Queen, Ross Schipper, William Yslas Vélez, by Sunder Lal, R. L. McFarland, and R. W. K. Odoni, and by M. Pohst.

The principles of *noncommutative arithmetics* are dealt with by Wilhelm Plesken and by Hans Zassenhaus.

The *geometry of numbers*, an ally of number theoretical research since Gauss and Dirichlet, which was developed as a new mathematical science by Hermite and Minkowski, is represented by the article of R. P. Bambah and A. C. Woods.

The *algebraic geometry of curves* providing a rich field of investigation in the spirit of number theory is dealt with in the contribution of Manohar L. Madan and Sat Pal. An application in the same spirit on the *theory of formal power series* is given by Charles F. Osgood.

Biographical Sketches

Henry B. Mann

In 1975 Henry B. Mann celebrated his seventieth birthday. A mathematician of international fame, Mann, in a career of more than forty years, has made significant contributions to algebra, number theory, statistics, and combinatorics.

Henry Mann was born October 27, 1905, in Vienna. He received his Ph.D. degree in mathematics in 1935 from the University of Vienna where, as a student of Philipp Furtwängler, he wrote his dissertation in algebraic number theory. After a year of teaching school in Vienna and a couple of years spent in research and tutoring, he emigrated in 1938 to the United States.

In New York he earned his living for several years primarily by tutoring. He had by then developed an interest in mathematical statistics, particularly in the analysis of variance, and in the problem of designing experiments with a view to their statistical analysis. He later contributed to this subject in a number of research papers and in his book (1949) "Analysis and Design of Experiments."

One of Mann's most remarkable achievements was his discovery in 1941 of a proof of a celebrated conjecture of Schnirelmann and Landau in additive number theory. This conjecture had its origin in the work of L. Schnirelmann in the early 1930s. Schnirelmann had considered a density $\delta(A)$ for a set of positive integers A, which he defined by

$$\delta(A) = \inf\{A(n)/n \mid n = 1, 2, \ldots\},$$

where $A(n)$ is the number of positive integers $\leq n$ in the set A. He showed

(most easily) that if the sum $A + B$ of two sets of positive integers is formed by $A + B = \{a, b, a + b | a \in A, b \in B\}$, then the density satisfies the rules:

(1) $\delta(A + B) \geq \delta(A) + \delta(B) - \delta(A)\delta(B)$.
(2) $A + B$ contains all positive integers if $\delta(A) + \delta(B) \geq 1$.

From these two rules he obtained (readily) the result that *any set having positive density is a basis for the integers* (that is, if $\delta(A) > 0$, then the sum of A with itself sufficiently many times contains all positive integers). As an application of these ideas, Schnirelmann proved (for the first time) the existence of a value k such that every integer greater than 1 is the sum of at most k primes. This he did by showing that $P + P—P$ is the set of primes together with 1—has positive density, hence is a basis for the integers.

Out of further study of these ideas by Schnirelmann himself and by E. Landau, there arose the conjecture that (1) and (2) may be replaced by the much stronger statement: *Either $A + B$ contains all positive integers or*

$$\delta(A + B) \geq \delta(A) + \delta(B).$$

This conjecture, appealing in its apparent simplicity, soon attracted wide attention. Many distinguished mathematicians attempted to find a proof; indeed, partial results were obtained over the next decade by E. Landau, A. Khintchine, A. Besicovitch, I. Schur, and A. Brauer.

It was this conjecture that Mann succeeded in proving in 1941. His interest in the problem had been aroused through the lectures of A. Brauer at New York University. Actually, he proved the still sharper statement: *If $C = A + B$, then either $C(n) = n$ or*

$$\frac{C(n)}{n} \geq \min \frac{A(m) + B(m)}{m}, \qquad 1 \leq m \leq n, \quad m \notin C.$$

For his proof he was awarded the Cole Prize in Number Theory by the American Mathematical Society in 1946. The technique that Mann introduced in his proof, and its various modifications, have led to further important results in additive number theory and have also proved useful in the more general setting of additive problems in groups.

In 1942 Mann was the recipient of a Carnegie Fellowship for the study of statistics at Columbia University. At Columbia he had the opportunity of working with Abraham Wald in the department of economics, which at that time was headed by Harold Hotelling. He taught for a year (1943–1944) in the Army Specialized Training Program at Bard College; he spent a year (1944–1945) as research associate at Ohio State University, and six months as research associate at Brown University. In 1946 he returned to Ohio State to join the mathematics faculty where, as associate professor (1946–1948) and full professor (1948–1964), he was actively engaged in teaching and research for many years. He held professorships at the University of Wiscon-

sin Mathematics Research Center from 1964 to 1971, and at the University of Arizona from 1971 until his retirement in 1975.

Mann's research interests in algebra and combinatorics cover a wide range. He has a special fondness, though, for algebraic number theory and Galois theory, and has imparted his enthusiasm for these subjects to many students over the years. Besides his dozen or so papers that contribute directly to these subjects, several of his papers on difference sets and coding theory contain beautiful applications of theorems on algebraic numbers and Galois theory.

Neither Henry Mann's research nor, for that matter, his teaching have ended with his retirement; he spent the past spring term as visiting professor at Oregon State University. He and his wife Anne, who this year observed their 41st wedding anniversary, plan to continue living in Tucson, Arizona.

His friends, colleagues, and students wish him many more years of good health and enjoyment of mathematics.

JOHN OLSON

BIBLIOGRAPHY OF HENRY B. MANN

RESEARCH ARTICLES

1. Ein Satz über Normalteiler, *Anz. Österreich. Akad. Wiss. Math.-Naturwiss. Kl.* (1935), Nr. 6, 49–50.
2. Über eine notwendige Bedingung für die Ordnung einfacher Gruppen, *Anz. Österreich. Akad. Wiss. Math.-Naturwiss. Kl.* (1935), Nr. 19, 209–210.
3. Untersuchungen über Wabenzellen bei allgemeiner Minkowskischer Metrik, *Mh. Math. Phys.* **42** (1935), 417–424.
4. Über die Erzeugung von Darstellungen von Gruppen durch Darstellungen von Untergruppen, *Mh. Math. Phys.* **46** (1937), 74–83.
5. A proof of the fundamental theorem on the density of sums of sets of positive integers, *Ann. of Math.* **43** (1942), 523–527.
6. On the choice of the number of class intervals in the application of the chi square test, *Ann. Math. Stat.* **13** (1942), 306–317 (with A. Wald).
7. The construction of orthogonal Latin squares, *Ann. Math. Stat.* **13** (1942), 418–423.
8. Quadratic forms with linear constraints, *Amer. Math. Monthly* **50** (1943), 430–433.
9. On stochastic limit and order relationships, *Ann. Math. Stat.* **14** (1943), 217–226 (with A. Wald).
10. On the statistical treatment of linear stochastic difference equations, *Econometrica* **11** (1943), 173–220 (with A. Wald).
11. On the construction of sets of orthogonal Latin squares, *Ann. Math. Stat.* **14** (1943), 401–414.
12. On orthogonal Latin squares, *Bull. Amer. Math. Soc.* **50** (1944), 249–257.
13. On certain systems which are almost groups, *Bull. Amer. Math. Soc.* **50** (1944), 879–881.
14. On a problem of estimation occurring in public opinion polls, *Ann. Math. Stat.* **16** (1945), 85–90. [A correction appears in *Ann. Math. Stat.* **17** (1946), 87–88.]
15. On a test for randomness based on signs of differences, *Ann. Math. Stat.* **16** (1945), 193–199.
16. Note on a paper by C. W. Cotterman and L. H. Snyder, *Ann. Math. Stat.* **16** (1945), 311–312.
17. Nonparametric tests against trend, *Econometrica* **13** (1945), 245–259.

18. Correction of G–M counter data, *Phys. Rev.* **68** (1945), 40–43 (with J. D. Kurbatov).
19. A note on the correction of Geiger Müller counter data, *Quart. J. Mech. Appl. Math.* **4** (1946), 307–309.
20. On a test of whether one of two random variables is stochastically larger than the other, *Ann. Math. Stat.* **18** (1947), 50–60 (with D. R. Whitney).
21. Integral extensions of a ring, *Bull. Amer. Math. Soc.* **55** (1949), 592–594 (with H. Chatland).
22. On the field of origin of an ideal, *Canad. J. Math.* **2** (1950), 16–21.
23. On the number of integers in the sum of two sets of positive integers, *Pacific J. Math.* **1** (1951), 249–253.
24. On the realization of stochastic processes by probability distributions in function spaces, *Sankhyā* **11** (1951), 3–8.
25. The estimation of parameters in certain stochastic processes, *Sankhyā* **11** (1951), 97–106.
26. On simple difference sets, *Sankhyā* **11** (1951), 357–364 (with T. A. Evans).
27. On products of sets of group elements, *Canad. J. Math.* **4** (1952), 64–66.
28. Some theorems on difference sets, *Canad. J. Math.* **4** (1952), 222–226.
29. On the estimation of parameters determining the mean value function of a stochastic process, *Sankhyā* **12** (1952), 117–120.
30. An addition theorem for sets of elements of Abelian groups, *Proc. Amer. Math. Soc.* **4** (1953), 423.
31. Systems of distinct representatives, *Amer. Math. Monthly* **60** (1953), 397–401 (with H. J. Ryser).
32. On the moments of stochastic integrals, *Sankhyā* **12** (1953), 347–350 (with A. P. Calderón).
33. On integral closure, *Canad. J. Math.* **6** (1954), 471–473 (with H. S. Butts and M. Hall, Jr.).
34. On an exceptional phenomenon in certain quadratic extensions, *Canad. J. Math.* **6** (1954), 474–476.
35. A generalization of a theorem of Ankeny and Rogers, *Rend. Circ. Mat. Palermo* **3** (1954), 106–108.
36. A theory of estimation for the fundamental random process and the Ornstein Uhlenbeck process, *Sankhyā* **13** (1954), 325–350.
37. On the efficiency of the least square estimates of parameters in the Ornstein Uhlenbeck process, *Sankhyā* **13** (1954), 351–358 (with P. B. Moranda).
38. Corresponding residue systems in algebraic number fields, *Pacific J. Math.* **6** (1956), 211–224 (with H. S. Butts).
39. On integral bases, *Proc. Amer. Math. Soc.* **9** (1958), 167–172.
40. A note to the paper "On integral bases" by H. B. Mann, *Proc. Amer. Math. Soc.* **9** (1958), 173–174 (with V. Hanly).
41. Some applications of the Cauchy–Davenport theorem, *Norske Vid. Selsk. Forh.* (*Trondheim*) **32** (1959), 74–80 (with S. Chowla and E. G. Straus).
42. The algebra of a linear hypothesis, *Ann. Math. Stat.* **31** (1960), 1–15.
43. A refinement of the fundamental theorem on the density of the sum of two sets of integers, *Pacific J. Math.* **10** (1960), 909–915.
44. Intrablock and interblock estimates, *in* "Contributions to Probability and Statistics," pp. 293–298. Stanford Univ. Press, Stanford, California, 1960 (with M. V. Menon).
45. On modular computation, *Math. Comput.* **15** (1961), 190–192.
46. An inequality suggested by the theory of statistical inference, *Illinois J. Math.* **6** (1962), 131–136.
47. On the number of information symbols in Bose–Chaudhuri codes, *Information and Control* **5** (1962), 153–162.
48. Main effects and interactions, *Sankhyā Ser. A* **24** (1962), 185–202.
49. Balanced incomplete block designs and Abelian difference sets, *Illinois J. Math.* **8** (1964), 252–261.
50. On the casus irreducibilis, *Amer. Math. Monthly* **71** (1964), 289–290.

51. Decomposition of sets of group elements, *Pacific J. Math.* **14** (1964), 547–558 (with W. B. Laffer).
52. On multipliers of difference sets, *Canad. J. Math.* **17** (1965), 541–542 (with R. L. McFarland).
53. Difference sets in elementary Abelian groups, *Illinois J. Math.* **9** (1965), 212–219.
54. On linear relations between roots of unity, *Mathematika* **12** (1965), 107–117.
55. Recent advances in difference sets, *Amer. Math. Monthly* **74** (1967), 229–235.
56. On canonical bases of ideals, *J. Combinatorial Theory Ser.* 0 **2** (1967), 71–76 (with K. Yamamoto).
57. Sums of sets in the elementary Abelian group of type (p, p), *J. Combinatorial Theory* **2** (1967), 275–284 (with J. E. Olson).
58. Two addition theorems, *J. Combinatorial Theory* **3** (1967), 233–235.
59. Properties of differential forms in n real variables, *Pacific J. Math.* **21** (1967), 525–529 (with J. Mitchell and L. Schoenfeld). [A correction appears in *Pacific J. Math.* **23** (1967), 631.]
60. On the p-rank of the design matrix of a difference set, *Information and Control* **12** (1968), 474–488 (with F. J. MacWilliams).
61. On orthogonal m-pods on a cone, *J. Combinatorial Theory Ser.* 0 **5** (1968), 302–307.
62. A new proof of the maximum principle for doubly-harmonic functions, *Pacific J. Math.* **27** (1968), 567–571 (with J. Mitchell and L. Schoenfeld).
63. On canonical bases for subgroups of an Abelian group, *in* "Combinatorial Mathematics and its Applications" (Proc. Conf., Univ. North Carolina, Chapel Hill, 1967), 38–54. Univ. of North Carolina Press, Chapel Hill, 1969.
64. A note on balanced incomplete block designs, *Ann. Math. Stat.* **40** (1969), 679–680.
65. On multipliers of difference sets, *Illinois J. Math.* **13** (1969), 378–382 (with S. K. Zaremba).
66. On the difference between the geometric and the arithmetic mean of n quantities, *Advances in Math.* **5** (1970), 472–473 (with C. Loewner).
67. Linear equations over a commutative ring, *J. Algebra* **18** (1971), 432–446 (with P. Camion and L. S. Levy).
68. Antisymmetric difference sets, *J. Number Theory* **4** (1972), 266–268 (with P. Camion).
69. Representations by kth powers in $GF(q)$, *J. Number Theory* **4** (1972), 269–273 (with G. T. Diderrich).
70. A necessary and sufficient condition for primality, and its source, *J. Combinatorial Theory Ser. A.* **13** (1972), 131–134 (with D. Shanks).
71. Combinatorial problems in finite Abelian groups, *in* "A Survey of Combinatorial Theory" (Proc. Internat. Symp. Combinatorial Math. and Its Appl., Colorado State Univ., Fort Collins, Colo., 1971), pp. 95–100. North-Holland, Amsterdam, 1973 (with G. T. Diderrich).
72. On Hadamard difference sets, *in* "A Survey of Combinatorial Theory" (Proc. Internat. Symp. Combinatorial Math. and Its Appl., Colorado State Univ., Fort Collins, 1971), pp. 333–334. North-Holland, Amsterdam, 1973 (with R. L. McFarland).
73. Prüfer rings, *J. Number Theory* **5** (1973), 132–138 (with P. Camion and L. S. Levy).
74. Additive group theory—a progress report, *Bull. Amer. Math. Soc.* **79** (1973), 1069–1075.
75. The solution of equations by radicals, *J. Algebra* **29** (1974), 551–554.
76. On normal radical extensions of the rationals, *Linear and Multilinear Algebra* **3** (1975), 73–80 (with W. Y. Veléz).
77. Prime ideal decomposition in $F(\sqrt[n]{\mu})$, *Monatsh. Math.* **81** (1976), 131–139 (with W. Y. Veléz).

BOOKS

1. "Analysis and Design of Experiments." Dover, New York, 1949.
2. "Introduction to Algebraic Number Theory." Ohio State Univ. Press, Columbus, 1955.
3. "Addition Theorems: The Addition Theorems of Group Theory and Number Theory." Wiley (Interscience), New York, 1965.

Arnold E. Ross

The following is a quotation from an address in honor of

Arnold E. Ross

at the Meeting of the Ohio Section of the Mathematical Association of America at Youngstown, Ohio, May 7, 1976

Tonight we are here to honor Arnold E. Ross, the man, the mathematician, and the leader of men.

We are very glad to have Arnold and Bee with us. She has been his companion in everyday's perplexities and his pillar of strength.

Born in Chicago in 1906 to an immigrant couple from southern Russia, Arnold was taken by his mother back to the old country in his early youth for a visit with his grandparents. The first World War and then the revolution cut them off from the USA for many years. He received most of his precollege education in Odessa, a cultured city on the Black Sea which provided the early environment of many famous scientists, musicians, and politicians.

Early influences are most formative and of the greatest impact on the intellectual development of a person and on the direction of his life work.

Arnold must have been a precocious youngster since he was able to enter the University under a special arrangement at less than sixteen years of age. It was Professor Shatunovsky who was deeply interested in very gifted youngsters and who was a friend of Arnold Ross' physician uncle who

encouraged this early start and helped with the needed arrangements. Besides Arnold, a cousin of his as well as one of his friends and another future mathematician, Felix Gantmacher, took part in the program, all of about the same boyish age. S. O. Shatunovsky (1859–1929), a distinguished Russian mathematician and educator, was one of the leaders of science and mathematics education in postrevolutionary Russia. Another prominent leader of science education in the 1930s in Russia was the energetic physicist Peter Kapitza (1894b.).

A small number of farsighted distinguished Russian scientists and mathematicians building on a centuries old excellent academic tradition succeeded in the twenties and thirties in designing and implementing a broadly based, competitive system of science and mathematics education in the elementary and secondary schools of the USSR, succeeding thereby in creating many more opportunities for the talented children of all sectors of the people than there had been available in czarist Russia.

In this country, Arnold's summer program for gifted high school students and a few other similarly oriented programs amply demonstrated in the sixties and seventies that a sizeable number of boys and girls at an age of 13 or slightly older are at the peak of their learning power, full of curiosity and eagerness to explore new avenues of thought, ready to be lead by skillful teachers much further than is presently possible at the high schools of this country.

Hungary and Belgium also have long traditions of talent search and nurture from which Arnold and his helpers have profited.

I can testify about a similar experience in Germany, where my parents sent me to a new school founded in Hamburg, Germany, a few years after the first World War, by a group of teachers who believed in "unlimited horizons" of learning for boys and girls between 10 and 18. Though the science and math training at the Lichtwarck Schule was no different from the traditional fare of other Hamburgian schools, in all other subjects—languages, music, art and handcraft, history and government, art appreciation, and philosophy—we received far more stimulation and we were given a good many more opportunities of independent studies than were available to other Hamburgian high school students.

The blessings of early nurture of intellectual curiosity by the careful attention of excellent teachers make the recipients desirous of conferring similar blessings on the next generation.

When Arnold came to Chicago in 1922 he was ready to study; but he first went to an engineering school and only in 1925 he enrolled in the study of higher mathematics at the University of Chicago.

I know many other colleagues whose love of mathematics was kindled while they were studying engineering. Raoul Bott started out as an engineer-

ing student and so did Hans Schwerdtfeger. At the University of Chicago Arnold fell under the spell of E. H. Moore (1862–1932), the well-known mathematician, educator, and organizer. It was of course E. H. Moore's problem-oriented method of teaching by self-discovery that left its permanent imprint on his mind as it is bound to influence everybody who has ever come under its spell.† On the basis of the earlier experience at the University of Odessa the new experience served as a catalyst for what became visible many years later. Shatunovsky and Moore both pioneered the directed limit generalization of the limit concept of analysis; both were very influential educational organizers and leaders in their great countries.

Arnold E. Ross graduated Ph.D. under L. E. Dickson in 1931. Subsequently he published a number of deep researches on the arithmetical properties of ternary quadratic forms. The big unsolved question remains whether a real ternary indefinite quadratic form that is bounded away from zero must be proportionate to a rational form.

Two postdoctoral years were spent at the California Institute of Technology, 1931–1933, where E. T. Bell and E. Bateman were active at that time. The next two years saw Arnold teaching mathematics at the Chicago City College Cooperative College, an academic self-help effort of the depression years which must have presented its organizers with quite a variety of nontrivial teaching problems.

Arnold spent his early academic career at the Department of Mathematics of the University of St. Louis at St. Louis, Missouri 1935–1946. In those years there was ample time to discuss all the problems of a small, but lively department of mathematics as well as the problems of higher mathematics and science education in a new country with colleagues like S. Warshawsky and G. Szegö and visitors like E. Artin, all three of them recent immigrants from Europe.

Following the European tradition, Arnold always took a strong interest in the sciences, in particular in modern physics. It was because of his friendship with C. Mullins and J. Guth that in 1946 they suggested to Father Kavanaugh, the president of the University of Notre Dame, Indiana, to ask Arnold E. Ross to succeed Karl Menger as the chairman of the Mathematics Department. One of the first things the new chairman did, as Arnold once told me, was to change the alphabetic listing of the freshman class lists to grouping by experience and readiness to study. He went in person to the President to achieve this change by force of his conviction. I think this little anecdote is characteristic of the length to which Professor Ross is likely to go for his students.

† See F. Browder, "Youthful enjoyment of rigorous thinking," *University of Chicago Magazine*, Winter 1975; and A. E. Ross, A preliminary report on a talent search program at the University of Chicago, November 1975.

One of his first Notre Dame students was Charles Misner, now a famous theoretical physicist and cosmologist who profited much from the ambitious undergraduate honors program developed jointly by A. E. Ross and C. Mullins.

During his 28 years as Chairman of the Department of Mathematics of the Notre Dame University (1946–1963) and The Ohio State University (1963–1974) Arnold E. Ross built up from inconspicuous beginnings a cornucopia of original training programs reflecting the essence of his own early experiences at Odessa and Chicago that talent is everywhere, it only needs to be nurtured lovingly to come to fruition.

Let me describe these programs in their fully developed form.

1. *Summer program for gifted high school students* (1964–1974 OSU, 1975 University of Chicago; ongoing; some NSF support; idea of program spreading to India and Australia, generating strong interest in Germany).

"Is community affluence a necessary prerequisite for early excellence? No, also small urban or rural communities, even the heart of the city communities harbours early excellence, it only must be developed" [13].

From a national reservoir of applications between 40 and 65 gifted boys and girls from the ages of 14 to 17 are selected for intensive on campus training by the best available teachers over a period of eight weeks for one, two, or three summers. Supervised housing is provided in campus dormitories. Former students of the program and other students act as counsellors and helpers for the young visitors who are under their care and supervision during the period of the training program.

I have often taught in these summer programs. The students I had there were my best ever. I could go as far with them (in essence) during a period of eight weeks as I could go with a normal graduate student class in the course of three quarters. I remember still vividly Mary, one of the gifted high school girls, sitting up on a tall tree in the middle of the Oval, deeply engaged in the study of a math book while everybody else basked in the warm summer sunshine.

The talented student brings as much to the program as he carries away!

Professor A. E. Ross discovered in a life long experience of discovery with his youngsters that *a course in elementary number theory is particularly suitable to test and develop the talents of a young gifted person.* Here follows a quotation from [14] regarding the objectives of the number theory training: "It is our aim to develop attitudes as well as skills, to introduce the students to an intelligent use of algorithms as well as to the mastery of the underlying theory, and to make use of number theory not only as an important stepping stone to the study of both analysis and algebra but also as an environment in which we can exhibit a whole gamut of vital dilemmas which confront any scientist in any field at one time or another.

"From the very beginning the student is given an opportunity to develop his powers of observation, to experiment, and to discover significant relations between the objects of his experimentation. The student learns to use the device of counterexamples to destroy the untenable conjectures, and as his experience grows he learns the meaning of providing the security of a proof for the surviving conjectures. As is natural in all fields of human activity the word labels follow recognition of phenomena, and the incentive for the precise and concise use of language comes from the desire and the need to share one's experience with others."

In the spirit of discovery so natural to all number theorists, and on the basis of the mathematical skills developed in the initial number theory course many other topics were taught successfully to those youngsters, e.g., mathematical logic (I. Thomas), geometry (J. Yaqub and H. Zassenhaus), linear algebra (Ledermann), algorithmic mathematics (H. Brown, H. Zassenhaus), combinatorics (D. Ray-Chaudhuri, N. Robertson, T. Dowling, and R. Wilson), analytic number theory (P. Turan), geometry of numbers (K. Mahler, A. Woods, P. Bambah, F. H. Davenport), advanced number theory (A. E. Ross), discrete groups (H. Zassenhaus), discrete geometry (A. Heppes). As in all other projects he accomplished, Arnold Ross used the principle "to match the talent of the teacher with the talent of the students."

2. *Academic Year Institute.* A strong program of training master teachers implemented at the University of Notre Dame 1960–1970 with NSF support.

Distinguishing features: Classes of not more than 20 selected mathematics teachers trained intensively during two summer periods of about six weeks each and an academic year between.

The choice of curriculum is guided by F. Klein's ideas on "elementary mathematics from the higher view point." Training offered in number theory (introductory), hard analysis (real and complex), linear algebra (geometric algebra), and geometry (affine and projective).

In my 1963 article† I reported about my experience of teaching geometric algebra while Y. Rainich was teaching the geometry. It is the renewal of commitment to basic mathematical ideas which distinguishes this program from an unstructured university program as well as from a program of studies in a college of education without the input of mathematicians. It is the three-phase nature of this particular program which gives it its depth. Of course the majority of the student participants continued their teaching career, as was the intention of the program. But many of them were placed into positions of increased administrative responsibility. About a third of the trainees went on to graduate Ph.D. at a number of universities and are now

† H. Zassenhaus, "The concept of depth in teacher training," *Amer. Math. Monthly* **70** (1963), 85–88.

in academic life. One graduate (Burt Kaufman), after an unusual academic and teaching career, founded a Federal laboratory for mathematical curriculum research and development which is now operating at St. Louis, Missouri.

3. *Proposal to upgrade the performance of graduate student assistants* (s. A. E. Ross, 1965) This became a living way of introducing the untutored incoming graduate student of mathematics at the Ohio State University into their subsequent course of more rigorous studies during the summers 1970–1974 by a specially designed summer program. It was always interesting to watch how the enthusiasm of the gifted high school students slowly infected the incoming graduate students, sometimes even the few older graduate students who were able to keep the pace of an ambitious eight week program.

4. *Basic algebra graduate course.* A new course originally taught by A. E. Ross (1967/68, 1968/69) to inexperienced incoming graduate students during the academic session. Based on lots of number theoretic examples the basic concepts of contemporary algebra are developed. The class is regrouped several times, and the top section is transformed in the course of the third quarter or in the subsequent summer quarter to a group of budding professional mathematicians.

For the three programs:

5. *Horizons Unlimited,*
6. *New Careers,* and
7. *Saturday Morning Program* cp. A. E. Ross, 1969, 1970. The Saturday morning classes started out as a Sunday class at Notre Dame University for local children who liked to be exposed to challenges of their mathematical inventiveness. For practical reasons the time of the weekly gatherings was changed to Saturday mornings. I have participated in this enterprise for several years; I was amazed at the distances boys and girls would travel (as far as from Gary to Notre Dame, or farther) to pick up additional information on regular polyhedra on rigid movements of the plane. Once, we spent nearly an hour on just discussing and illustrating the nature of the identity mapping interpreted as a rigid "motion."

Saturday morning classes are now being conducted by A. E. Ross and his staff in cooperation with the Columbus school system. The value of this kind of university input into the local community cannot be measured in terms of dollars and cents. Our environment becomes a better place to live in if it provides opportunities like the Saturday morning classes to all inquisitive persons.

In a long career leading from his 1931 graduation at the University of Chicago to the 1976 Summer Institute at the same University Professor

Arnold E. Ross developed and exercised his own talents as a teacher and "conductor" of the mathematical community.

His personal influence and the excellence of his building is much in evidence at the University of Notre Dame and at The Ohio State University and will remain so after his retirement. Through his Summer Institute, many gifted students of the State of Ohio as well as of every other State of the union and also of the Canadian provinces of Ontario and Quebec have profited immensely. What is more important, the ideas of Arnold E. Ross continue to develop their infectious quality in far away countries like Australia, India, and Germany, and his example and personal stimulation remain alive with colleagues like A. Woods, J. Yaqub, D. Ray-Chaudhuri, J. Riner, T. Ralley, and many others, including myself.

HANS ZASSENHAUS

BIBLIOGRAPHY OF A. E. ROSS

1. A note on three equivalent theorems, *Bull. Amer. Math. Soc.* **39** (1933), 204.
2. On representation of integers by ternary forms, *Bull. Amer. Math. Soc.* **38** (1932), 636–637.
3. On representation of integers by indefinite ternary quadratic forms of quadratfrei determinant, *Amer. J. Math.* **55** (1933), 293–302.
4. On representation of integers by quadratic forms, *Proc. Nat. Acad. Sci. U.S.A.* **18** (1933), 600–608.
5. Positive quaternary quadratic forms representing all but a finite number of integers, *Bull. Amer. Math. Soc.* **39** (1933), 510.
6. On criteria for universality of ternary quadratic forms, *Bull. Amer. Math. Soc.* **38** (1938), 632.
7. A theorem on simultaneous representation of primes and its corollaries, *Bull. Amer. Math. Soc.* **45** (1939), 899–906.
8. On a problem of Ramanujan, *Amer. J. Math.* **68** (1946), 29–46.
9. An extension of a Problem of Kloosterman, *Amer. J. Math.* **68** (1946), 59–65 (with Gordon Pall).
10. Proposal for a plan to upgrade the performance of graduate student assistants at The Ohio State University 1965 (unpublished).
11. Horizons Unlimited, Preprint 1969.
12. The shape of our tomorrows, *Amer. Math. Monthly* **77** (1970), 1002–1007.
13. Nature or Nurture; December 1973. A report on the student science-training summer program sponsored by the National Science Foundation and by the Ohio State University.
14. Fostering Scientific Talent (1973), pp. 71–77, Chapter five.
15. Chairman's Report, The National Research Council, Committee on Undergraduate Education (1974).

Olga Taussky-Todd

At the age of about 15 (a pupil of the only Mittelschule for girls in Linz, Upper Austria) I came to realize that science and mathematics were to be my subjects. Slowly this changed to "mainly mathematics," with science still of great interest to this day, and in due course mathematics meant mainly number theory.

I became a student of the University of Vienna where I received my doctoral degree, with a dissertation entitled "Über eine Verschärfung des Hauptidealsatzes." My supervisor was P. Furtwängler who had established the main facts about the Hilbert class field. Hilbert had himself stated these facts, based only on his research of relative quadratic extension fields. Only very few of Hilbert's statements were proved to be incorrect, among them was the statement that the class field had class number equal to 1. However, the weaker statement, the Hauptidealsatz, was proved correct during my student days by Furtwängler too, using the newly found technique of translating the assertion into a statement about finite groups with abelian commutator subgroups. With feasible problems in class field theory being very scarce Furtwängler was delighted to have plenty of thesis problems available now by using the same technique. His idea was to study the fields between the given field and the class field to see which and how many ideal classes of the ground field would become principal in such a field, i.e., a generalization of Hilbert's Theorem 94. Unfortunately, this did not turn out to be a good idea. The technique did not work well for the intermediate fields and the theorems seemed to be of a chaotic nature. The results

of my thesis problem made Furtwängler give up class field theory forever after. Artin called the problems hopeless. However, I myself returned to them in quite recent years, based on a group theoretic proof of Theorem 94 by M. Hall. I gave this new research the title "Hilbert's Theorem 94," and several, mainly young people, have contributed toward it. At the time of my recent Ph.D., however, I made only two further contributions which had a certain influence many years later. One was my collaboration, mainly by correspondence, with A. Scholz on our investigation of Theorem 94 for relative cubic unramified extension fields of a number of imaginary quadratic fields. In this case exactly one class becomes principal (a fact that Scholz denoted as "capitulation"). Further, we examined the group theoretic possibilities for the group of the second class field for fields with 3-class group with two basis elements, assuming that only one ideal class becomes principal. The second contribution concerned a group theoretic proof for the fact that for the 2-class group a group of type (2, 2), the class field has an odd class number. This fact, the result of the joint work with Scholz, and the fact that a cyclic p-class group always leads to a class field with class number prime to p, led to a conjecture concerning group towers whose positive answer would have implied that every class field tower is finite. However, the group tower conjecture was defeated on group theoretic grounds and finally Šafarevič (together with Golod) showed the existence of an infinite group tower for a numerical case.

Among other subjects of particular interest during my student days was the work of Menger on metric geometry and mathematical logic. I obtained some results on the former subject and participated in the Wiener Kreis led by Schlick.

During the following years I obtained a position at the Mathematics Institute of Göttingen University as one of the editors of Hilbert's work in number theory and then returned to Wien as assistant to Hahn and Menger. I supervised a thesis on multiply monotone sequences, learning functional analysis in this way. At that time two important changes happened to me. On the mathematical side I became interested in topological algebra and "sums of squares," on the career side I obtained a scholarship at Bryn Mawr College and a fellowship at Girton College, Cambridge, England. Topological algebra came to me via Pontrjagin's work on topological fields and some fascinating problems posed by van der Waerden in the *Jahresber. deutsch. Math. Vereini.* In a joint paper Jacobson and I generalized Pontrjagin's work to locally compact rings, and I published the first topological proof (via spheres) of Frobenius' theorem concerning hypercomplex systems over the reals which are also division algebras. Later I proved that the Laplace differential equations in n dimensions for n functions can be deduced

from generalized Cauchy–Riemann equations only for $n = 1, 2, 4, 8$. This was reproved by Stiefel and plays a certain role in combinatories now.

Jobs were very scarce in Great Britain then, even for British-born people and even more for the many foreigners taking refuge there. I obtained a junior teaching position in the University of London. It was then that I met John Todd (Jack) employed in a similar position at King's College, University of London. We got married in 1938.

In due course the war broke out and life became very difficult, e.g., we had to move 18 times during the war. The first year of the war was spent at Belfast where I supervised a young theologian, E. Best, who was also very much interested in mathematics. Jointly we started on the investigation of finite groups for which the concept of "normal subgroup" is transitive. This came about through a suggestion of John Todd. This work was continued in Italy (Zacher, Zappa) and in Germany (Gaschütz, Huppert). During my time in Belfast I was cut off from my own mathematical papers, but the library of Queen's University there was very helpful to my needs. I saw there among other things the papers of McCoy on matrices with property P and the papers of Latimer and MacDuffee on classes of matrices. Both these rather different basic sets of ideas have stayed with me ever since and have led to substantial research on my part. I will come back to this soon.

My London college moved to Oxford during the war, a city expected to be safe from air raids. However, life there was very complicated because of the shortage of housing for just the reason of safety. In some ways I preferred living in London in spite of the bomb danger. My teaching duties became heavier, but not more interesting. My husband had a scientific research job with the British Admiralty in Portsmouth and later in London. I myself obtained a research job with the Ministry of Aircraft Production in 1943. It was there that I became fully interested in matrix theory for I worked in the so-called Flutter Group, under the matrix expert R. A. Frazer. It was impossible not to come under the spell of matrix theory in that group. My interest in bounds for characteristic roots of matrices, in particular in Geršgorin's theorem and in criteria for stable matrices, arose out of this phase of my life. To this I will return. However, I myself was asked to work on boundary value problems for hyperbolic differential equations arising from flutter at supersonic speed on which Temple had already made progress. There were new problems, and my particular problem was mentioned in Hadamard's book, "Théorie des Ondes," in a footnote, as not arising in practical work. After a long struggle I managed to solve it and I published it after the war in a book dedicated to Courant on his 60th birthday.

In 1947 my husband accepted an invitation to the USA to the National Bureau of Standards to work toward the exploitation of high speed elec-

tronic computing machines which were under construction then. I accompanied him and was soon employed myself there. Our chief, John H. Curtiss, had much understanding for my professional possibilities.

During this year we were allowed to spend one term at the Institute for Advanced Study where we were appointed as members. We were attached to the von Neumann group. It was there that I started to shake off my wartime weariness and also my wartime research interests. The latter, however, were still helpful in my work at the National Bureau of Standards where we were called back a year later and where we stayed altogether for 10 years. Although I was given much freedom there, on the whole, I was supposed to devote myself to problems that could be applied to practical work. I accepted part-time payment, partly to be able to return to number theory, partly to avoid the fixed civil service hours. During my time at Princeton I had contacts with Artin, Chowla, Reiner, Schafer, among others. In particular a conversation with Chowla brought me back to the theorems of Latimer and MacDuffee on classes of matrices. At the end of my stay I gave a lecture at Harvard on my boundary value problem and then proceeded to Los Angeles, to work with Jack at the newly opened Institute for Numerical Analysis (INA), a field station of the National Bureau of Standards at UCLA. After a very cold winter in Princeton the California climate helped to restore me even more and my new research interests became even clearer to me: eigenvalues of polynomials in several matrices on the one hand, integral matrices on the other. For the first a suggestion by Mark Kac was most helpful. It was the definition of the L-property (L for linear) for pairs of matrices. This property means that in the pencil generated by the pair, the eigenvalues are linear functions. When the very gifted mathematician T. S. Motzkin joined INA, I told him of my partial results. We soon started on joint publications and proved some general facts on matrices with multiple eigenvalues in a pencil and a theorem (suggested to us by Kaplansky) concerning a pencil in which every matrix is diagonable. Motzkin introduced methods of algebraic geometry into this subject. I myself realized its close connection to complex function theory; Kato reproved our result via perturbation methods and included it in his big book on this subject. Later on I published further work on the L-property by myself and suggested problems to others.

I have at all times suggested problems to others, and I had even published several in the section on research problems in the *Bulletin*. Five of those led to published research. One of them concerned the infinite Hilbert matrix. This matrix does not have π as an eigenvalue if only vectors in the usual Hilbert space are admitted. However, I suggested to prove that π was still an eigenvalue for vectors outside this space. This was shown by Kato and further elaborated by M. Rosenblum.

While still at the Bureau of Standards, I continued research on the theorem of Latimer and MacDuffee and started work on units in the integral group ring. I became interested in this via Higman's thesis. Later I treated them via unimodular group matrices. I introduced M. Newman into this subject, and we published several papers on it; I was particularly concerned with the positive definite case.

In 1957 we both accepted positions at California Institute of Technology and it seemed to me as if an odyssey of 20 years (I left Cambridge, England in 1937) had ended. I could at last work again with academic freedom and have Ph.D. students. I had eleven there. At the National Bureau of Standards I had one only, K. Goldberg, attached to the close-by American University. He worked on the Hausdorff formula. Otherwise I worked with several postgraduates like A. J. Hoffman and with visitors: Ostrowski, Wielandt, K. Fan, H. Cohn, J. C. P. Miller, P. Stein, Stiefel.

When still at the National Bureau of Standards I was able to use a theorem by Shoda which I had cherished for a long time. It concerned matrices with trace $= 0$ or $\det = 1$. Now at Caltech my student R. C. Thompson generalized this theorem to all possible fields. Another student, C. Hobby, with the help of Zassenhaus, contributed greatly to the solution of the class field tower problem. His work was completed by Serre.

Several scholars of immense power came to Caltech during my stay and worked with me a great deal. After years of frequent isolation from mathematicians working in my line, or sometimes from mathematicians altogether, sometimes in positions with hard duties, this was most beneficial for me. These were particularly in number theory Zassenhaus, Dade, and A. Froehlich. They were really interested in my problems on integral matrices and raised my understanding of my own ideas. Unfortunately, in previous times, even with brilliant mathematicians as colleagues I could not force myself to break away from my own problems, even if my progress was frustrating at times. Even in my student days I was alone in my number theoretic work. In Europe in the old days one did not call on one's supervisor freely. However, this attitude helped me to develop my own problems. In recent years a young man Kisilevsky has been a brilliant colleague. In any case working with the gifted Caltech students is a great stimulus.

Again, at Caltech, like at the Bureau of Standards, the chairman of the department, Frederic H. Bohnenblust, set up my job to give me much freedom.

I want to return to my work on matrices at Caltech. I continued on the L-property, but still stimulated by my experience in aerodynamics I made progress on the algebraic treatment of Lyapunov's stability criterion. This led to considerable work by others. Here I obtained much stimulus from W. Givens and from H. Schneider. My contacts with the powerful matrix

school of Marvin Marcus are very beneficial at all times. Work with Wielandt who visited Caltech was also very beneficial.

Apart from work on the L-property I was active in other parts of matrix theory, other generalizations of commutativity, and in particular commutators. The thesis of Gaines fits in here; that of Parker is in another area of matrix theory.

At times work on matrices leads to analogous investigations in number theory and for real matrices. This was evident in my own work in two different areas: (1) Positive definite real symmetric or hermitian matrices. Here, e.g., my work connected with the Lyapunov theorem and two theses (C. Johnson, R. Loewy) fits in. On the other hand, in number theory I worked on positive definite group matrices (i.e., integral "symmetric," "positive definite" group ring elements) and on integral symmetric matrices (this is linked to positive definite similarity). For the rational case there is the E. Bender thesis, recently greatly extended by him. (2) Factorization into symmetric factors (thesis of Uhlig) for real matrices and into integral symmetric matrices for integral matrices (so far mainly for $n = 2$) by myself. This last work is linked with norms from quadratic fields, as well as in my quite recent work on rational 2×2 commutators $AB - BA$.

Among my matrix work there is a commutator result on which I made some observations in a paper of 1961 (with elegant follow-up by Zassenhaus) which seems to have stimulated analysts like De Prima and his students, Putnam, and Berberian, although its origin is from classical finite group theory. It concerns unitary matrices whose eigenvalues lie on less than a semicircle, called cramped matrices now.

While I myself found no occasion to return to the Geršgorin theorem, my early light contributions and problems were taken up by several colleagues, in particular A. J. Hoffman, P. Henrici, J. Todd, and R. S. Varga, who arrived at important results.

Of my other number theory students—L. Foster, D. Davis, and D. Maurer—the first two based their investigations on tables obtained by computers. I myself have been much interested in computational number theory, a subject in which my co-author A. Scholz—mentioned earlier—was a master. For my work on integral 2×2 matrices the tables of E. L. Ince on class groups and units in real quadratic fields are a wonderful help.

Among other results obtained during my Caltech time is a "sum of squares" result, concerning a new 8-square identity. This was generalized by Eichhorn and Zassenhaus to a 16-square identity.

BIBLIOGRAPHY OF OLGA TAUSSKY-TODD

1. Zur Metrik der Gruppen, *Anz. Österreich Akad. Wiss. Math.-Natur. Kl.* **15** (1930), 1–3.
2. Über Pseudo-G-Quadrupel, *Math. Z.* **33** (1931), 412–415.
3. Über eine Verschärfung des Hauptidealsatzes, *Jber. Deutsch. Math. Verein.* (1931).
4. Zur Theorie des Klassenkörpers, *Jber. Deutsch. Math. Verein.* **41** (1932), 74.
5. On similarity of groups, *Ann. of Math.* **32** (1931), 754–755.
6. Über eine Verschärfung des Hauptidealsatzes, *Crelles J.* **168** (1932), 193–210.
7. Über isomorphe Abbildungen von Gruppen, *Math. Ann.* **198** (1933), 615–620.
8. Zur Axiomatik der Gruppen, *Ergebnisse eines math. Kolloquiums Wien*, **4** (1933), 2–3.
9. Die Hauptideale der kubischen Klassenkörper imaginär-quadratischer Zahlkörper, ihre rechnerische Bestimmung und ihr Einfluss auf den Klassenkörperturm, *Crelles J.* **171** (1934), 19–41 (with A. Scholz).
10. Editor of "Hilbert's Collected Papers," Vol. I (Theory of numbers), J. Springer, Berlin, 1932.
11. Editor of "Hilbert's Collected Papers," Vol. II (Theory of invariants, algebra, geometry), J. Springer, Berlin, 1933.
12. Editor of E. Artin's lectures on class field theory, Göttingen, 1932.
13. Locally compact rings, *Proc. Nat. Acad. Sci. U.S.A.* **21** (1935), 106–108 (with N. Jacobson).
14. Abstrakte Körper und Metrik, *Ergebnisse eines math. Kolloquiums Wien*, **6** (1935), 20–23.
15. Zur topologischen Algebra, *Ergebnisse eines math. Kolloquiums Wien*, **7** (1936), 60–61.
16. Analytical methods in hypercomplex systems, *Compositio Math.* **3** (1936), 399–407.
17. Some problems of topological algebra, abstract of a paper given at the International Congress of Mathematicians at Oslo, 1936.
18. A remark on the class field tower, *J. London Math. Soc.* **12** (1937), 82–85.
19. On unramified class fields, *J. London Math. Soc.* **12** (1937), 85–88.
20. Über Schiefringe, *Sitzungsber. Akad. Wiss. Wien* **38** (1937), 145 (with P. Furtwängler).
21. Rings with non-commutative addition, *Bull. Calcutta Math. Soc.* **38** (1936), 245–246.
22. An algebraic property of Laplace's differential equation, *Quart. J. Math. Oxford Ser.* **10** (1939), 99–103.
23. Matrices with finite period, *Proc. Edinburgh Math. Soc.* **6** (1940), 128–134 (with J. Todd).
24. A characterisation of algebraic numbers, *Proc. Roy. Irish Acad. Sect.* **46A** (1940), 1–8 (with J. Todd).
25. Determinants of quaternions, *Bull. Amer. Math. Soc.* **46** (1940), 431–432 (with J. Todd).
26. Matrices of finite period, *Proc. Roy. Irish Acad. Sect.* **46A** (1941), 113–121 (with J. Todd).
27. Inversion in groups, *Quart. J. Math. Oxford Ser.* **12** (1941), 65–67 (with J. Todd).
28. A class of groups, *Proc. Roy. Irish Acad. Sect.* **47A** (1942), 55–62 (with E. Best).
29. Infinite powers of matrices, *J. London Math. Soc.* **17** (1943), 146–151 (with J. Todd).
30. Professor David Hilbert, For. Mem. R.S., Obituary *Nature (London)* **152** (1943), 182.
31. A note on skew-symmetric matrices, Aeronautical Research Committee Reports and Memoranda 2006, 1944.
32. Some aspects of modern algebra, *Science Progress* (1947), 253–268 (with J. Todd).
33. A method for obtaining bounds for characteristic roots of matrices with applications to flutter calculations, Aeronautical Research Council of Great Britain, Report 10.508, 1947.
34. On some boundary value problems in the theory of the non-uniform supersonic motion of an aerofoil, Aeronautical Research Committee Reports and Memoranda 2141, (1947).
35. A boundary value problem for hyperbolic differential equations arising in the theory of the non-uniform supersonic motion of an aerofoil, *in* "Courant Anniversary Volume," pp. 421–435, Interscience, New York, 1948.
36. Covering theorems for groups, *Annales de la Société Polonaise de Mathématique* **21** (1948), 303–305 (with J. Todd).

37. Note on a theorem in n-dimensional geometry, *Amer. Math. Monthly* **55** (1948), 471–494 (with L. A. Wigglesworth).
38. Bounds for characteristic roots of matrices, *Duke Math. J.* **15** (1948), 1043–1044.
39. On a theorem of Latimer and MacDuffee, *Canad. J. Math.* **1** (1949), 30–302.
40. A remark concerning the characteristic roots of the finite segments of the Hilbert matrix, *Quart. J. Math. Oxford Ser.* **20** (1949), 80–83.
41. A recurring theorem on determinants, *Amer. Math. Monthly* **56** (1949), 672–676.
42. Note on the condition of matrices, MTAC **4** (1950), 111–112.
43. Classes of matrices and quadratic fields, *Pacific J. Math.* **1** (1951), 127–132.
44. Bounds for characteristic roots of matrices II, *J. Res. Nat. Bur. Stand.* **46** (1951), 124–125.
45. Arnold Scholz zum Gedaechtnis, *Math. Nachr.* **7** (1952), 379–386.
46. Classes of matrices and quadratic fields II, *J. London Math. Soc.* **27** (1952), 237–239.
47. Matrices with property L, *Trans. Amer. Math. Soc.* **73** (1952), 108–114 (with T. S. Motzkin).
48. Bibliography on bounds for characteristic roots of finite matrices, NBS Report 1162, 1951.
49. On the variation of a positive definite matrix, *Proc. Akad. Wet. Amsterdam* **54** (1951), 383–385 (with A. Ostrowski).
50. Classes of matrices and quadratic fields, Proc. Int. Cong. of Mathematicians, 1950.
51. Editor of NBS Applied Mathematics Series 29, Simultaneous linear equations and the determination of eigenvalues, 1952 (reprinted 1958).
52. Editor of NBS Applied Mathematics Series 39, Contributions to the solution of systems of linear equations and the determination of eigenvalues, 1954.
53. Systems of equations, matrices and determinants, *Math. Mag.* Sept.–Oct. 1952, 9–20, and Nov.–Dec. 1952, 71–88. (Now part of "The Tree of Mathematics", Digest Press, Pacoima, California, 1957) (with J. Todd).
54. Generalized commutators of matrices, *in* "Studies in mathematics and mechanics presented to R. von Mises," pp. 67–68, Academic Press, New York, 1954.
55. Pairs of matrices with property L (II) *Trans. Amer. Math. Soc.* **82** (1955), 387–401 (with T. S. Motzkin).
56. Characteristic roots of quaternion matrices, *Arch. Math. (Basel)* **5** (1954), 99–101.
57. A characterization of normal matrices, *J. Res. Nat. Bur. Stand.* **52** (1954), 17–19 (with A. J. Hoffman).
58. On representations of finite groups, *Proc. Akad. Wet. Amsterdam, Ser. A* **55** (1952), 511–513 (with T. S. Motzkin).
59. Review of "Sur quelques propriétés des valeurs caractéristiques des matrices carrées" by M. Parodi, *Proc. Amer. Math. Soc.* **59** (1958), 464.
60. Pairs of matrices with property L, *Proc. Nat. Acad. Sci. U.S.A.* **39** (1953), 961–963 (with T. S. Motzkin).
61. Some computational problems in algebraic number theory, *Proc. Amer. Math. Soc. Sixth Symposium on Applied Mathematics*, held at Santa Monica, City College, August 1953, 1956.
62. Discrete analogs of inequalities of Wirtinger, *Monatsh. Math.* (1955), 73–90 (with K. Fan and J. Todd).
63. Generation and testing of pseudo-random numbers, in "Symposium on Monte Carlo Method" (H. A. Meyer, ed.) pp. 15–28, Wiley, New York, 1956 (with J. Todd).
64. Normal matrices in some problems in algebraic number theory, Proc. Inter. Math. Cong., Amsterdam, Sept., 1954.
65. On the number of absolute points of a correlation, *Pacific J. Math.* **6** (1956), 83–96 (with A. J. Hoffman, M. Newman, and E. G. Straus).
66. On a generalization of the normal basis in abelian algebraic number fields, *Comm. Pure Appl. Math.* **9** (1956), 85–91 (with M. Newman).

67. Unimodular integral circulants, *Math. Z.* **63** (1955), 285–289.
68. A note on group matrices, *Proc. Amer. Math. Soc.* **6** (1955), 984–986.
69. Abstract of "Matrix Methods in Algebraic Number Theory," Pasadena, Calif., 1955.
70. Remark on the preceding paper: algebraic equations satisfied by roots of natural numbers, *Pacific J. Math.* **6** (1956), 97–98 (with E. G. Straus).
71. An algebraic proof of the isoperimetric inequality for polygons, *J. Wash. Acad. Sci.* **45** (1955), 339–342 (with K. Fan and J. Todd).
72. Review of "Economic activity analysis" (O. Morgenstern, ed.), Wiley, New York, (1954), *Bull. Amer. Math. Soc.* **61** (1955), 241–243.
73. Commutators of A and A^*, *J. Wash. Acad. Sci.* **46** (1956), 38–40 (with T. Kato).
74. Classes of positive definite unimodular circulants, *Canad. J. Math.* **9** (1957), 71–73 (with M. Newman).
75. Commutativity in finite matrices, *Amer. Math. Monthly* **65** (1957), 229–235.
76. Commuting bilinear transformation and matrices, *J. Wash. Acad. Sci.* **46** (1956), 373–375 (with J. Todd).
77. Application of quaternions to the representations of a binary quadratic form as a sum of four squares, *Proc. Roy. Irish Acad. Sect.* **58A** (1957), 23–28 (with G. Pall).
78. Some computational problems involving integral matrices, *J. Res. Nat. Bur. Stand.* **65** (1961), 15–17.
79. On matrix classes corresponding to an ideal and its inverse, *Illinois J. Math.* **1** (1957), 108–113.
80. Review of "Mathematical Methods for Digital Computers," by A. Ralston and H. S. Wilf, Econometrica, **29** (1961), 487.
81. On a determinantal inequality of H. P. Robertson, *I. Proc. Wash. Acad. Sci.* (1958), 263–264.
82. On a matrix theorem of Craig and Hotelling, *Proc. Akad. Wet. Amsterdam, Ser. A* **61** (1958), 137–141.
83. Research problems, *Bull. Amer. Math. Soc.* **64** (1958), 124.
84. Some discrete variable computations, *Proc. Symp. Appl. Math.*, Amer. Math. Soc. Comb. Anal., vol. 10, 1960, pp. 201–209 (with J. Todd).
85. Chapters on algebra, ordinary differential equations, operators, *in* "Handbook of Physics" (E. U. Condon, and H. Odishaw, eds.), McGraw-Hill, New York, 1958, rev. second ed. 1967.
86. A note on the group commutator of A and A^*, *J. Wash. Acad. Sci.* **48** (1959), 305.
87. On the similarity transformation between a matrix and its transpose, *Pacific J. Math.* **9** (1959), 893–896 (with H. Zassenhaus).
88. Matrices of rational integers, *Amer. Math. Bull.* **66** (1960), 327–345.
89. A weak property L for pairs of matrices, *Math. Z.* **71** (1959), 463–465.
90. The quadratic subfield of the field generated by the pth root of unity, *Amer. Math. Monthly* **67** (1960), 769.
91. Commutators of unitary matrices which commute with one factor, *J. Math. Mech.* **10** (1961), 175–178.
92. Some remarks concerning the real and imaginary parts of the characteristic roots of a finite matrix, *J. Mathematical Physics* **1** (1960), 234–236 (with D. C. Lewis, Jr.).
93. A remark on a theorem of Lyapunov, *J. Math. Anal. Appl.* **2** (1961), 105–107.
94. Research problem, *Bull. Amer. Math. Soc.* **66** (1960), 275.
95. Review of "Computational Methods of Linear Algebra" by V. N. Faddeeva, Dover. *Math. Gaz.* **44** (1960), 139–140.
96. Chapter on bounds for eigenvalues of finite matrices, *in* "Survey of Numerical Analysis" (J. Todd, ed.), McGraw-Hill, New York, 1962.

97. On the semigroup of ideal classes in an order of an algebraic number field, *Bull. Amer. Math. Soc.* **67** (1961), 305–308 (with E. C. Dade and H. Zassenhaus).
98. Linear relations between higher commutators, *Proc. Amer. Math. Soc.* **13** (1962), 732–735 (with H. Wielandt).
99. On the matrix function $AX + X'A'$, *Arch. Rational Mech. Anal.* **9** (1962), 93–96 (with H. Wielandt).
100. Matrices with trace zero, *Amer. Math. Monthly* **69** (1962), 40–42.
101. A generalization of a theorem of Lyapunov. *J. SIAM* **9** (1961), 640–643.
102. A characterization of property L, *J. Math.* **41** (1962), 291–293.
103. On the theory of orders, in particular on the semigroups of ideal classes and genera of an order in an algebraic number field, *Math. Ann.* **148** (1962), 31–64 (with E. C. Dade and H. Zassenhaus).
104. Ideal Matrices I, *Arch. Math.* **13** (1962), 275–282.
105. On the role of the determinant in semigroups of matrices, *Quart. J. Math. Oxford Ser.* **14** (1963), 123–130 (with H. Wielandt).
106. Ideal Matrices II, *Math. Ann.* **150** (1963), 218–225.
107. On the different in orders in an algebraic number field and special units connected with it, *Acta Arith.* **9** (1964), 47–51 (with E. C. Dade).
108. Divisors of recurrent sequences, *Crelles J.* **214/15** (1964), 180–183 (with E. C. Dade, D. W. Robinson, M. Ward).
109. On the Variation of the Characteristic Roots of a Finite Matrix Under Various Changes of its Elements, *in* "Recent Advances in Matrix Theory," pp. 125–138. Univ. Wisconsin Press, Madison, Wisconsin, 1964.
110. Some new results connected with matrices of rational integers, *Proc. Symp. Pure Math. American Math. Soc.* **8** (1965), 78–88 (with E. C. Dade).
111. Matrices C with $C^n \to 0$, *J. Algebra* **1** (1964), 5–10.
112. Scalar matrix quadratic residues, *Mathematika* **12** (1965), 94–96 (with G. Pall).
113. Revised 85.
114. 3 Problems in Matrix Theory, *Bull. Amer. Math. Soc.* **71** (1965), 711.
115. Positive definite matrices, *in* "Inequalities" (Oved Shisha, ed.), pp. 309–319. Academic Press, New York, 1967.
116. A determinantal identity for quaternions and a new eight square identity, *J. Math. Anal. Appl.* **15** (1966), 161–164.
117. Remarks on a matrix problem arising in statistics. *Monatsh. Math.* **70** (1966), 461–464.
118. On the similarity transformation between an integral matrix with irreducible characteristic polynomial and its transpose, *Math. Ann.* **166** (1966), 60–63.
119. Integral matrices, Lectures at National Science Foundation Seminar on Algebraic Number Theory, Bowdoin College, 1966.
120. Stable Matrices 75–88, "Programmation en mathématiques numériques" Colloques Internationaux du CNRS, No. 165, Editions du CNRS, Paris, 1968.
121. Gershgorin and his circles ... (with J. Todd, R. S. Varga), in preparation.
122. The factorization of the adjugate of a finite matrix, *Linear Algebra and Appl.* **7** (1968), 39–41.
123. The discriminant matrices of an algebraic number field, *J. London Math. Soc.* **43** (1968), 152–154.
124. Positive definite matrices and their role in the study of the characteristic roots of general matrices, *Advances in Math.* **2** (1968), 175–186.
125. Automorphs and generalized automorphs of quadratic forms treated as characteristic value relations, *Linear Algebra and Appl.* **1** (1968), 349–356.

126. (1, 2, 4, 8)-sums of squares and Hadamard matrices, *Proc. Symp. Pure Math. Combinatorics* **19**, 229–233, *Amer. Math. Soc. 1971.*
127. On the 1-cohomology of the general and special linear groups, *Aequationes Math.* **5** (1970), 129–201 (with H. Zassenhaus).
128. A generalization of matrix commutativity, *Linear Algebra and Appl.* **2** (1969), 349–353.
129. Zbirovi Kvadrata, *Matematicka Biblioteka (Belgrade, Yugoslavia)* **41** (1969), 19–27.
130. Special problems concerning the GL(n, F) and SL(n, F), Lecture at NSF Seminar in Algebraic Groups, Bowdoin College, 1968.
131. On two matrices, problem, *SIAM Review* **10** (1968), 379.
132. Factorization of Cayley numbers, *J. Number Theory* **2** (1970), 74–90 (with G. Pall).
133. A remark concerning Hilbert's Theorem 94, *J. Reine Angew. Math.* **239/240** (1970), 435–438.
134. Some computational problems in Number Theory, *Bull. Inst. Math. Appl.* **6** (1970), 29–30.
135. Hilbert's Theorem 94, "Computers in Number Theory," pp. 65–71. Academic Press, New York, 1971.
136. Sums of squares, *Amer. Math. Monthly* **77** (1970), 805–830.
137. Automorphs of quadratic forms as positive operators, *Proc. 3rd Symp. Inequalities*, 1969, *in* "Inequalities III (O. Shisha, ed.), pp. 341–345, Academic Press, 1972.
138. Some remarks on ad A, *in* "Studies in Pure Mathematics," pp. 235–237, Academic Press, 1971.
139. A remark concerning the similarity of a finite matrix A and A^*, *Math. Z.* **117** (1970), 170–189.
140. The role of symmetric matrices in the study of general matrices, *Linear Algebra and Appl.* **5** (1972), 147–154.
141. Problems on matrices and operators, *Bull. Amer. Math. Soc.* **76** (1970), 977.
142. Some results concerning the transition from the L- to the P-property for pairs of finite matrices, *J. Algebra* **20** (1972), 271–283.
143. Hilbert's theorem 90 in matrix rings, *Linear and Multilinear Algebra* **1** (1973), 5–8.
144. A result concerning classes of matrices, *J. Number Theory* **6** (1974), 64–71.
145. The factorization of an integral matrix into two integral symmetric matrices I, abstract of a lecture at Baton Rouge, *Conf. Quadratic Forms*, March 1972.
146. The factorization of an integral matrix into two integral symmetric matrices II, Summary of a lecture at Boulder number theory meeting, August 1972.
147. The factorization of an integral matrix into two integral symmetric matrices I, *Acta Arith.* **24** (1973), 151–156.
148. The factorization of an integral matrix into two integral symmetric matrices, *Bull. Amer. Math. Soc.* **79** (1973), 956–958.
149. The factorization of an integral matrix into two integral symmetric matrices II, *Comm. Pure Appl. Math.* **26** (1973), 847–854.
150. Two research problems, *Linear and Multilinear Algebra* **1** (1973), 173.
151. Pairs of matrices having property L, *Gatlinburg V Symp. Numerical Algebra*, June 1972.
152. Research problems, *Linear and Multilinear Algebra* **1** (1973), 273.
153. Additive commutators between 2×2 integral matrix representations of orders in identical or different quadratic number fields, *Bull. Amer. Math. Soc.* **80** (1974), 885–887.
154. Response to Query 26, *Notices Amer. Math. Soc.* **21** (1974), 159.
155. Additive commutators of rational 2×2 matrices, *Linear Algebra and Appl.* **12** (1975), 1–6.
156. Some results concerning the transition from the L- to the P-property for pairs of finite matrices II, *Linear and Multilinear Algebra* **2** (1974), 195–202.
157. A matrix approach to a computational problem of Gauss in number theory, abstract, *Gatlinburg VI Symp. Numerical Algebra*, December 1974.

158. Two facts concerning rational 2×2 matrices leading to integral ternary forms representing zero, Seminar Notes CIT 1976.
159. Norms in quadratic fields and their relation to non commuting 2×2 matrices I, *Monatsh. Math.*, **82** (1976), 282–283.
160. Editor of Seminar Notes in Number Theory 1974/75, selected topics on ternary forms and norms, Calif. Inst. Tech., Pasadena, 1976.
161. Solution of Problem for *Amer. Math. Monthly* (jointly with H. Zassenhaus), to appear.
162. From Pythagoras theorem via sums of squares to celestial mechanics, Sigma Xi lecture, May 1975, to be published.
163. Some modern work on determinants, invited address at San Francisco, Mathematical Association of America, January 1974, in preparation.
164. Commutativity and generalized commutativity of finite matrices, invited lecture at Santa Barbara *Conf. Finite Matrices*, December 1973, in preparation.
165. History of Sums of Squares in Algebra, invited lecture at El Paso History of Algebra Conference, November 1975, to appear in *Graduate Studies*, Texas Tech. University, Lubbock, Texas.
166. Norms in quadratic fields related to noncommuting rational 2×2 matrices, Resumé for Kyoto Conference, March 1976.
167. Norms from quadratic fields and their relation to non-commuting 2×2 matrices II. The principal genus, to appear in *Houston J. Math.*
168. Norms from quadratic fields and their relation to non-commuting 2×2 matrices III. A link between the 4-rank of the ideal class groups in $Q(\sqrt{m})$ and in $Q(\sqrt{-m})$, to appear in *Math. Zeitschr.*

Number Theory and Algebra

Octaves and Modular Forms

BRAM VAN ASCH

RIJKSUNIVERSITEIT UTRECHT
UTRECHT, THE NETHERLANDS

We consider a lattice L in an octave algebra V, and an even integral quadratic form q, defined on L. It will be shown that $\sum_{a \in L,\, q(a)=n} (a^{2k}, e)$ is $O(n^{k+3})$ if $k = 1, 2, 3$, and is $O(n^{k+3/2+\varepsilon})$ for any $\varepsilon > 0$ if $k \geqslant 4$.

Introduction

It is known that the number of variables of an even integral quadratic form with determinant unity must be divisible by 8. It is also known that there is, up to equivalence, exactly one such form of eight variables. We consider an octave algebra V over the field of real numbers, the underlying space of which is an eight-dimensional real vector space, equipped with a (multiplicative) norm q: $V \to \mathbb{R}$. A scalar product on V is defined by $(x, y) = q(x + y) - q(x) - q(y)$. It will turn out that we can choose a lattice $L \subset V$ such that q defines on L an even integral quadratic form with determinant unity. Let F be a spherical function with respect to q. By a theorem due to Schoeneberg (see [3]) we know that the theta series

$$\Theta(\tau; F) = \sum_{a \in L} F(a) e^{2\pi i \tau q(a)}$$

(where τ is a complex variable whose imaginary part is positive) is a modular

form of weight $(4 + \deg(F))$ for the full modular group. If $\deg(F) > 0$, it is even a cusp form. Define for any positive integer k

$$A_k(n) = \sum_{a \in L,\ q(a)=n} (a^k, e), \qquad n \geqslant 0.$$

If k is odd we have $A_k(n) = 0$. We will consider $A_{2k}(n)$. It will be shown that by choosing special spherical functions F we obtain a relation between $A_{2k}(n)$ and the coefficients of certain cusp forms. This will enable us to prove†

Theorem *For any* $\varepsilon > 0$

$$A_{2k}(n) = p_k n^k \sigma_3(n) + O(n^{k+3/2+\varepsilon}),$$

where $p_1 = -360$, $p_2 = 144$, $p_3 = -24$, *and* $p_k = 0$ *for all* $k \geqslant 4$.

In fact, this theorem states that for $k \geqslant 4$ the geometrical distribution of the $2k$th powers of octaves in L of norm n is utterly dissimilar to this distribution for $k \leqslant 3$.

The contents are as follows. First we recall some facts about spherical functions, most of which may be found in Hecke [2, pp. 849–853]. Next we describe how x^{2k} can be expressed in terms of x and (the unit element) e, and finally the proof will be carried out.

1. Let V be a finite-dimensional real vector space of even dimension $2n$, and let $(,)$: $V \times V \to \mathbb{R}$ be a scalar product. We write $q(x) = \frac{1}{2}(x, x)$ for any $x \in V$. A homogeneous polynomial function F is said to be a spherical function with respect to q if

$$\frac{\partial^2 F}{\partial x_1^2} + \cdots + \frac{\partial^2 F}{\partial x_{2n}^2} = 0, \qquad \text{where} \quad x = x_1 e_1 + \cdots + x_{2n} e_{2n}$$

for some orthonormal basis $e_1, \ldots, e_{2n}$ of V. Hecke [2, p. 853] has shown that we can obtain all spherical functions of degree k by taking linear combinations of the polynomials

$$(q(x)q(y))^{k/2} H_k\left(\frac{(x, y)}{2\sqrt{q(x)q(y)}}\right)$$

for all parameters $y \in V$. Here H_k is a polynomial in one variable T satisfying the differential equation

$$(1 - T^2)\frac{d^2 H_k}{dT^2} - (2n - 1)T\frac{dH_k}{dT} + k(2n + k - 2)H_k = 0. \tag{1}$$

† This question was raised by F. van der Blij.

From

$$\int_{-1}^{1} H_k(T)H_l(T)(1-T^2)^{n-3/2}\,dT = 0 \qquad \text{if} \quad k \neq l \tag{2}$$

it is easy to deduce that $H_k(T)$ is up to a scalar multiple equal to

$$\frac{1}{(1-T^2)^{n-3/2}}\frac{d^k}{dT^k}[(1-T^2)^{k+n-3/2}]. \tag{3}$$

We normalize H_k such that the coefficient of T^k is equal to 1. In particular we get

$$H_0(T) = 1, \qquad H_1(T) = T, \qquad H_2(T) = T^2 - \frac{1}{2n},$$

$$H_3(T) = T^3 - \frac{6n+3}{(2n+1)(2n+2)}T.$$

We shall need only spherical functions of even degree $2k$. We have, for $k \geqslant 1$,

$$H_{2k}(T) = T^{2k} - \omega_{2k} + \sum_{j=1}^{2k-1} \gamma_{j,2k}H_j(T), \tag{4}$$

where $\gamma_{j,2k} = 0$ if j is odd. Using (2) we can determine the constant ω_{2k}. We have

$$0 = \int_{-1}^{1} H_{2k}(T)H_0(T)(1-T^2)^{n-3/2}\,dT = \int_{-1}^{1} (T^{2k} - \omega_{2k})(1-T^2)^{n-3/2}\,dT,$$

which implies

$$\omega_{2k} = \frac{\Gamma(k+\frac{1}{2})\Gamma(n)}{\Gamma(k+n)\Gamma(\frac{1}{2})}. \tag{5}$$

2. Let $V = \mathbb{R}^8$, considered as an algebra of octaves. As a general reference for octaves we use Coxeter [1]. Let e_i, $1 \leqslant i \leqslant 8$, be the standard basis for V, and let the multiplication in V be fixed such that $e_1 = e$ is the unit element of V. We define for $x = (x_1, \ldots, x_8) \in V$, $q(x) = x_1^2 + \cdots + x_8^2$.

The following formula holds:

$$x^2 = (x, e)x - q(x)e. \tag{6}$$

Furthermore q is multiplicative, i.e.,

$$q(xy) = q(x)q(y). \tag{7}$$

From (6) we can easily deduce that $x^{2k} = P_{2k}x + Q_{2k}e$, where P_{2k} and Q_{2k} are polynomials in the two variables $X = (x, e)$ and $Y = q(x)$. We have $P_2(X, Y) = X$, $Q_2(X, Y) = -Y$.

The following recursion formulas hold

$$P_{2k} = X^2 P_{2k-2} - YP_{2k-2} + XQ_{2k-2}, \qquad Q_{2k} = -XYP_{2k-2} - YQ_{2k-2}. \tag{8}$$

We conclude from (8) that P_{2k} and Q_{2k} must be of the form

$$\begin{aligned} P_{2k}(X, Y) &= \sum_{l=0}^{k-1} \alpha_{2l,\,2k} X^{2k-2l-1} Y^l, \\ Q_{2k}(X, Y) &= Y \sum_{l=0}^{k-1} \beta_{2l,\,2k} X^{2k-2l-2} Y^l. \end{aligned} \tag{9}$$

By induction it can easily be proved that

$$\alpha_{2l,\,2k} = (-1)^l \binom{2k-l-1}{l}$$

and

$$\beta_{2l,\,2k} = (-1)^{l+1} \binom{2k-l-2}{l}, \qquad 0 \leqslant l \leqslant k-1. \tag{10}$$

For convenience we put $\alpha_{2l,\,2k} = 0 = \beta_{2l,\,2k}$ if $l < 0$ or $l \geqslant k$. We get

$$(x^{2k}, e) = \sum_{l=0}^{k} [\alpha_{2l,\,2k} + 2\beta_{2l-2,\,2k}](x, e)^{2k-2l} q(x)^l. \tag{11}$$

3. Let $R \subset V$ be the subset

$$R = \{\pm e_i \pm e_j \mid 1 \leqslant i < j \leqslant 8\} \cup \left\{ \frac{1}{2} \sum_{i=1}^{8} (-1)^{v(i)} e_i \;\middle|\; \sum_{i=1}^{8} v(i) \text{ even} \right\}.$$

R is a root system of type E_8. Let L be the lattice generated in V by $\frac{1}{2}\sqrt{2}\,R$. A straightforward calculation shows that $q(L) \subset \mathbb{Z}$, and q defines on L a quadratic form with determinant unity. It may be found in Hecke [2, p. 868] that for any positive integer n

$$\#\{a \in L \mid q(a) = n\} = 240\sigma_3(n), \tag{12}$$

where $\sigma_3(n) = \sum_{d|n} d^3$.

Now we take $F_{2k}(x) = q(x)^k H_{2k}((x, e)/2\sqrt{q(x)})$, a spherical function of degree $2k$. We know that $\Theta(\tau; F_{2k})$ is a cusp form of weight $4 + k$. We define

$$B_{2k}(n) = \sum_{a \in L,\, q(a)=n} F_{2k}(a) = n^k \sum_{a \in L,\, q(a)=n} H_{2k}\left(\frac{(a, e)}{2\sqrt{n}}\right).$$

Since there are no nonzero cusp forms of weight 6, 8, 10, we have

$$B_2(n) = B_4(n) = B_6(n) = 0. \tag{13}$$

By (4) and (12) we get

$$B_{2k}(n) = \frac{1}{2^{2k}} \sum_{a \in L} (a, e)^{2k} + \sum_{l=1}^{k-1} \gamma_{2l,\,2k} n^{k-l} B_{2l}(n) - 240 n^k \omega_{2k} \sigma_3(n),$$

which implies

$$\sum_{a \in L,\, q(a)=n} (a, e)^{2k} = \sum_{l=1}^{k} \delta_{2l,\,2k} n^{k-l} B_{2l}(n) + 240 n^k 2^{2k} \omega_{2k} \sigma_3(n)$$

for some constants $\delta_{2l,\,2k}$, $1 \leqslant l \leqslant k$. Substituting this in (11) yields

$$A_{2k}(n) = \sum_{l=0}^{k-1} \sum_{j=1}^{k-l} [\alpha_{2l,\,2k} + 2\beta_{2l-2,\,2k}] \delta_{2j,\,2k-2l} n^{k-j} B_{2j}(n)$$

$$+ 240 n^k \sigma_3(n) \sum_{l=0}^{k} [\alpha_{2l,\,2k} + 2\beta_{2l-2,\,2k}] 2^{2k-2l} \omega_{2k-2l}.$$

Suppose now $k \geqslant 4$ and consider the last sum. By (5) and (10) this sum equals

$$\sum_{l=0}^{k} (-1)^l \frac{12k(2k-l-1)!}{l!\,(k-l+3)!\,(k-l)!}$$

$$= \frac{12(k-4)!}{(k-1)!} \sum_{l=0}^{k} (-1)^l \binom{k}{l} \binom{2k-l-1}{k-4} = 0,$$

as can easily be proved by writing $T^{k-1}(1+T)^k = \sum_{l=0}^{k} \binom{k}{l} T^{2k-l-1}$, differentiating both sides $k-4$ times, and substituting $T = -1$. So $A_{2k}(n)$ is a combination of $n^{k-j} B_{2j}(n)$, provided $k \geqslant 4$, and since the $B_{2j}(n)$ are coefficients of cusp forms of weight $j+4$, this establishes the part of the theorem for $k \geqslant 4$.

As for $k = 1, 2, 3$, it follows immediately from (13) that

$$A_2(n) = -360 n \sigma_3(n),$$

$$A_4(n) = 144 n^2 \sigma_3(n),$$

$$A_6(n) = -24 n^3 \sigma_3(n),$$

which establishes the remainder of the theorem.

REFERENCES

[1] H. S. M. Coxeter, Integral Cayley Numbers, *Duke Math. J.* **13** (1946), 561–578.
[2] E. Hecke, "Mathematische Werke." Vandenhoeck and Ruprecht, Göttingen, 1959.

[3] B. Schoeneberg, Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen, *Math. Ann.* **116** (1939), 511–523.

AMS (MOS) 1970 subject classifications: 10D05, 10E25, 17A30.

On the Product of Three Inhomogeneous Linear Forms

R. P. BAMBAH
PANJAB UNIVERSITY
CHANDIGARH, INDIA

A. C. WOODS†
THE OHIO STATE UNIVERSITY
COLUMBUS, OHIO

For $i = 1, 2, 3$ let $L_i = a_{i1}u_1 + a_{i2}u_2 + a_{i3}u_3$ be linear forms in the variables u_1, u_2, u_3 with real coefficients a_{ij} satisfying $\det(a_{ij}) = 1$. It is proved that given any real numbers c_1, c_2, c_3 there exist integral values of the variables u_1, u_2, u_3 such that simultaneously

$$\prod_{i=1}^{3} |L_i + c_i| \leqslant \tfrac{1}{4} \qquad \textit{and} \qquad L_1 + c_1 < 0.$$

1. Introduction

For $1 \leqslant i \leqslant n$, let $L_i = a_{i1}u_1 + \cdots + a_{in}u_n$ be n linear forms in the variables $u_1, \ldots, u_n$ with real coefficients a_{ij} satisfying $\det(a_{ij}) = 1$. A classical conjecture of Minkowski asserts that, given any real numbers $c_1, \ldots, c_n$, the inequality

$$\prod_{i=1}^{n} |L_i + c_i| \leqslant 2^{-n}$$

† The research of the second author was partially supported by National Science Foundation Grant GP43919.

has a solution in integral values of the variables. This has been proved only for $n \leqslant 5$; see Skubenko [4]. Stemming from this problem is the conjecture that, given any real numbers $c_1, \ldots, c_n$, the inequalities

$$\prod_{i=1}^{n} |L_i + c_i| \leqslant 2^{-n+1}, \qquad L_1 + c_1 < 0$$

have a common solution in integral values of the variables. This has been proved by Cole [2] in the case $n = 2$. Our aim is to present a proof in the case $n = 3$, using a method introduced by Birch and Swinnerton-Dyer [1].

Let $A_j = (a_{1j}, \ldots, a_{nj})$ for $1 \leqslant j \leqslant n$ and denote by Λ the lattice of basis $A_1, \ldots, A_n$ so that $d(\Lambda) = 1$. Set $m(\Lambda) = \inf |x_1 \cdots x_n|$ extended over all points $(x_1, \ldots, x_n)$ of Λ other than the origin O. Paralleling the work of Birch and Swinnerton-Dyer [1], it is sufficient to consider only those lattices whose homogeneous minimum $m(\Lambda)$ is positive and attained by some point of Λ provided it is shown that the strict inequality holds in this case. An alternative proof of this reduction will be given elsewhere using the divided cell technique. In what follows it is assumed that Λ has these properties.

2. The Main Lemmas

Let a be a positive real number with $a^3 \leqslant \frac{4}{7}$. Denote by K_1 the set of points (x, y) that satisfy an inequality of the form

$$|x|y_0 + |y|x_0 < 4/a$$

where x_0, y_0 are positive numbers with

$$x_0 + y_0 \leqslant \sqrt{\frac{14}{3}}a + 4\sqrt{\frac{3}{14}}\frac{1}{a^2} \qquad \text{and} \qquad x_0 y_0 = \frac{4}{a}.$$

Similarly, denote by K_2 the set of points (x, y) that satisfy

$$|x|y_0 + |y|x_0 < 4/a$$

where x_0, y_0 are positive numbers with

$$x_0 + y_0 \leqslant 4\sqrt{\frac{3}{7}}\frac{1}{a^2} \qquad \text{and} \qquad x_0 y_0 = \frac{4}{a}.$$

Put $\theta = 6(\sqrt{2} - 1)/7$.

Lemma 1 *Let L be a lattice in the plane with $d(L) = 4/a$ and such that no two points of L are less than a distance $\sqrt{\frac{14}{3}}$ a apart. Then there exist positive numbers ξ, η such that the parallelogram Π given by $|x|\eta + |y|\xi < 4/a = \xi\eta$ is L-admissible and lies in K_1 if $a^3 \geqslant \theta$, in K_2 if $a^3 \leqslant \theta$.*

Let S denote the set of points (x, y) such that there exists a half-open

interval I of length a for which $t \in I$ implies

$$(1) \quad |(x+t)(y+t)(t-a)| < 1 \qquad \text{and} \qquad (2) \quad t - a < 0.$$

Similarly, let S' denote the set of points (x, y) such that there exists a half-open interval I of length a for which $t \in I - \{0\}$ implies (1) and (2).

Lemma 2 (*a*) *If* $a^3 \geqslant \theta$, *then* $K_1 \subseteq S$ *and* $B(K_1) \subseteq S'$.
(*b*) *If* $a^3 \leqslant \theta$, *then* $K_2 \subseteq S$ *and* $B(K_2) \subseteq S'$.

3. Proof of the Theorem

Before proving these lemmas we show how the theorem follows. We first restate the theorem in a form convenient for our purpose. Let Λ be a lattice in R^3 with $d(\Lambda) = 4$. Again assume that the homogeneous minimum $m(\Lambda)$ is attained and nonzero.

Theorem *Given any real numbers* x_0, y_0, z_0, *there exists a point* (x, y, z) *of* Λ *such that*

$$|(x+x_0)(y+y_0)(z+z_0)| < 1 \qquad \textit{and} \qquad z + z_0 < 0.$$

Proof Let $X \in \Lambda$ be such that $m(\Lambda)$ is attained at $\pm X$. Applying a map of the form $x \to \lambda x$, $y \to \mu y$, $z \to |\lambda\mu|^{-1} z$, where $\lambda \neq 0$, $\mu \neq 0$, it is clear that we may assume either X or $-X$ is the point (a, a, a) where $a > 0$. By a well-known result of Davenport [3] it follows that (i) $a^3 \leqslant \frac{4}{7}$ and (ii) the projection L of Λ into the plane $z = 0$ parallel to the vector (a, a, a) is a lattice of determinant $4/a$ with no two of its points less than $\sqrt{\frac{14}{3}}\, a$ apart. By Lemma 1 there exist positive numbers ξ, η such that the parallelogram Π given by $|x|\eta + |y|\xi < 4/a = \xi\eta$ is L-admissible. By a classical result of Minkowski, any coplanar translates of Π and L either have a common point or their boundaries have at least two common points. The projection of $\Lambda + (x_0, y_0, z_0)$ onto the plane $z = -a$ parallel to the vector (a, a, a) yields a translate of L. Hence, either there exists a point $(x^*, y^*, -a)$ of this translate such that $(x^*, y^*) \in \Pi$, or there exist two distinct points $(x_1^*, y_1^*, -a)$, $(x_2^*, y_2^*, -a)$ of this translate such that (x_1^*, y_1^*) and (x_2^*, y_2^*) are on the boundary of Π. In the first case Lemma 2 implies that $(x^*, y^*) \in S$ and, since $(a, a, a) \in \Lambda$, the theorem is true. In the second case $(x_1^*, y_1^*) \in S'$ and $(x_2^*, y_2^*) \in S'$. By similar reasoning to that used in the first case, either the theorem is true or $(x_1^*, y_1^*, -a)$ and $(x_2^*, y_2^*, -a)$ both lie in $\Lambda + (x_0, y_0, z_0)$, which would immediately imply that $m(\Lambda) = 0$, the case we have excluded. This completes the proof of the theorem.

4. Proof of Lemma 1

Let c be the largest positive number such that the parallelogram P given by $|x| + |y| \leqslant c$ is L-admissible.

Case 1 $c \geqslant 2/\sqrt{a}$ Let Π be the parallelogram obtained by putting $\xi = \eta = 2/\sqrt{a}$ so that Π is L-admissible and $\xi\eta = 4/a$. Then

$$\xi + \eta = \frac{4}{\sqrt{a}} \leqslant \sqrt{\frac{14}{3}}a + 4\sqrt{\frac{3}{14}}a^{-2}$$

since $(a^{3/2} - 2\sqrt{\frac{3}{14}})^2 \geqslant 0$. Thus Π lies in K_1. If $a^3 \leqslant \theta$, then, since $\theta < \frac{3}{7}$,

$$4/\sqrt{a} \leqslant 4\sqrt{\tfrac{3}{7}}a^{-2}$$

and Π lies in K_2, which completes this case.

Case 2 $c < 2/\sqrt{a}$ Denote by (x^*, y^*) one of the points of L that necessarily lie on the boundary of P. The symmetry of the lemma allows us to suppose that $y^* \geqslant x^* \geqslant 0$. By hypothesis

$$x^{*2} + y^{*2} \geqslant \tfrac{14}{3}a^2.$$

Let ξ, η be positive numbers such that

(i) $\xi\eta = 4/a$,
(ii) $\xi \geqslant \eta$, and
(iii) the parallelogram Π given by $|x|\eta + |y|\xi < 4/a$ contains (x^*, y^*) on its boundary.

The existence of such a pair ξ, η follows from the fact that P contains (x^*, y^*) on its boundary and $c < 2/\sqrt{a}$. We claim that this choice of ξ, η satisfies the conclusion of Lemma 1. In the first place, Π is L-admissible, for otherwise Π contains a point of L linearly independent of (x^*, y^*) in its interior, which implies that $d(L) < 4/a$, a contradiction. Assume first that $a^3 \geqslant \theta$ and, by way of contradiction, that

$$\xi + \eta > \sqrt{\frac{14}{3}}a + 4\sqrt{\frac{3}{14}}a^{-2}.$$

Since $\xi\eta = 4/a$, $\xi \geqslant \eta$, $\sqrt{\frac{14}{3}}a4\sqrt{\frac{3}{14}}a^{-2} = 4/a$ and $4\sqrt{\frac{3}{14}}a^{-2} \geqslant \sqrt{\frac{14}{3}}a$ it follows that $\xi > 4\sqrt{\frac{3}{14}}a^{-2}$ and $\eta < \sqrt{\frac{14}{3}}a$.

The line $x\eta + y\xi = 4/a$ meets the line $x = y$ in the point $(4/a(\xi + \eta), 4/a(\xi + \eta))$ whose distance from O is

$$\frac{4\sqrt{2}}{a(\xi + \eta)} < \frac{4\sqrt{2}}{a(\sqrt{\frac{14}{3}}a + 4\sqrt{\frac{3}{14}}a^{-2})} \leqslant \sqrt{\frac{14}{3}}a$$

since $\theta \leqslant a^3$. Hence the line $x\eta + y\xi = 4/a$ meets the axis $x = 0$ and the line $x = y$ in points both less than a distance $\sqrt{\frac{14}{3}}a$ from O. Since $y^* \geqslant x^*$, this

does not permit (x^*, y^*) to lie on the boundary of Π, a contradiction. Therefore we may assume $a^3 \leqslant \theta$ and, by way of contradiction, that

$$\xi + \eta > 4\sqrt{\frac{3}{7}}\frac{1}{a^2}.$$

Put

$$\xi^* = \left(2\sqrt{\frac{3}{7}} + 2\sqrt{\frac{3}{7} - a^3}\right)\frac{1}{a^2}, \qquad \eta^* = \left(2\sqrt{\frac{3}{7}} - 2\sqrt{\frac{3}{7} - a^3}\right)\frac{1}{a^2}$$

so that, in particular, $\xi^*\eta^* = 4/a$, $\xi^* \geqslant \eta^*$, and $\xi^* + \eta^* = 4\sqrt{\frac{3}{7}}a^{-2}$. The line $x\eta^* + y\xi^* = 4/a$ meets the line $x = y$ in the point $(\sqrt{\frac{7}{3}}a, \sqrt{\frac{7}{3}}a)$ which is at distance $\sqrt{\frac{14}{3}}a$ from O. The same line meets $x = 0$ in the point $(0, 4/a\xi^*)$ whose distance from O is

$$\frac{4}{a\xi^*} \leqslant \sqrt{\frac{14}{3}}a$$

since $a^3 \leqslant \theta$. By the initial assumption, $\xi > \xi^*$ and $\eta < \eta^*$ and so the line $x\eta + y\xi = 4/a$ meets $x = 0$ and $x = y$ in points both less than a distance $\sqrt{\frac{14}{3}}a$ from O. Again this implies that (x^*, y^*) cannot lie on the boundary of Π, the contradiction that proves Lemma 1.

5. Proof of Lemma 2

Let $(x, y) \in \mathrm{CL}(K_1)$ if $a^3 \geqslant \theta \in \mathrm{CL}(K_2)$ if $a^3 \leqslant \theta$. Let x_0, y_0 be a pair of numbers that can be associated with x, y in the definition of K_1 and K_2 so that $|x|y_0 + |y|x_0 \leqslant 4/a = x_0 y_0$ and, therefore, by the arithmetic–geometric mean inequality

$$|xya| \leqslant 1 \tag{1}$$

with strict inequality unless (x, y) is not in either K_1 or K_2. Thus, if $|xya| = 1$, the hypothesis of the lemma allows us to exclude the value $t = 0$. We shall make repeated use of this fact in what follows without expressly calling attention to it. From the symmetry in x, y we may assume $|x| \leqslant |y|$. Further, $|y| \leqslant 4/ax_0 = y_0$, so that an upper bound for y_0 is also an upper bound for y. If $(x, y) \in \mathrm{CL}(K_1)$, then

$$y_0 \leqslant 4\sqrt{\tfrac{3}{14}}a^{-2} = (1.8516\ldots)a^{-2}.$$

On the other hand, if $(x, y) \in \mathrm{CL}(K_2)$, then

$$y_0 \leqslant (2\sqrt{\tfrac{3}{7}} + 2\sqrt{\tfrac{3}{7} - a^3})a^{-2} \leqslant 4\sqrt{\tfrac{3}{7}}a^{-2} = (2.6186\ldots)a^{-2}.$$

Thus, in either case, $y_0 \leqslant 4\sqrt{\frac{3}{7}}a^{-2}$.

Case A $x \leqslant 0$ Put $f(t) = (x + t)(y + t)(t - a)$. We shall show that if $0 < t < a$, then $|f(t)| < 1$. We distinguish cases:

(i) $x \leqslant -a$ In $f(t)$ the coefficient of t is $xy - ay - ax = c(t)$, say. If $y \leqslant 0$, then $c(t) > 0$ since all terms are nonnegative. If, however, $y > 0$, then $c(t) < 0$ since $|y| \geqslant |x|$. Hence $f(t)$ is monotone on $[0, a]$. Since $|f(0)| \leqslant 1$ and $f(a) = 0$, the result follows.

(ii) $-a \leqslant x \leqslant 0$ and $y > 0$ Again $c(t) < 0$ so that $f(t)$ is monotone decreasing on $[0, -x]$. Since $|f(0)| \leqslant 1$ and $f(-x) = 0$ it follows that $|f(t)| < 1$ on $(0, -x]$. On the other hand, if $t \in [-x, a)$, then

$$|f(t)| = |(t + x)(t + y)(t - a)| \leqslant \tfrac{1}{4}a^2(|y| + a) < 1.$$

(iii) $-a \leqslant x \leqslant 0$ and $y \leqslant 0$ Again $c(t) \geqslant 0$ so $f(t)$ is monotone increasing on $[0, -x]$ and, as before, $|f(t)| < 1$ when $t \in (0, -x]$. If $t \in [-x, a)$, we repeat the argument under (ii) to obtain $|f(t)| < 1$.

Case B $x \geqslant a$ $f(t)$ has a single extremum in $[-x, a]$ and therefore is monotone on at least one of the two intervals $[-x, 0]$ or $[0, a]$, and so the result follows as before.

We must now distinguish between the cases $a^3 \geqslant \theta$ and $a^3 \leqslant \theta$. Assume for the time being that $a^3 \geqslant \theta$ so that, in particular,

$$y_0 \leqslant 4\sqrt{\tfrac{3}{14}}\,a^{-2}.$$

Case C $0 \leqslant x \leqslant \frac{1}{2}a$ For $0 < t < a$ we have

$$\begin{aligned} |(x + t)(y + t)(t - a)| &= |y_0(x + t)x_0(y + t)(t - a)/x_0 y_0| \\ &\leqslant \tfrac{1}{4}(y_0(|x| + t) + x_0(|y| + t))^2 \tfrac{1}{4}a(a - t) \\ &\leqslant (a^{-1} + \tfrac{1}{4}t(\sqrt{\tfrac{14}{3}}\,a + 4\sqrt{\tfrac{3}{14}}\,a^{-2}))^2 a(a - t), \end{aligned}$$

and, putting $t = \lambda a$, so that $0 < \lambda < 1$ this is

$$(1 + \tfrac{1}{4}\lambda(\sqrt{\tfrac{14}{3}}\,a^3 + 4\sqrt{\tfrac{3}{14}}))^2(1 - \lambda) \leqslant (1 + s\lambda)^2(1 - \lambda) = g(\lambda), \quad \text{say,}$$

where $s = \frac{1}{7}\sqrt{\frac{14}{3}} + \sqrt{\frac{3}{14}} \leqslant .772$. Then $g'(\lambda) = (1 + s\lambda)(2s - 1 - 3s\lambda) < 0$ if $\frac{1}{2} \leqslant \lambda < 1$. Since $g(1) = 0$ and $g(\frac{1}{2}) < 1$, it follows that when $\frac{1}{2}a \leqslant t < a$ we do have

$$|(x + t)(y + t)(t - a)| < 1$$

as desired. Now suppose $0 < t \leqslant \frac{1}{2}a$, so that $0 < \lambda \leqslant \frac{1}{2}$. Put $x = \mu a$ so that $0 \leqslant \mu \leqslant \frac{1}{2}$. Then

$$|(x + t)(a - t)| = a^2(\lambda + \mu)(1 - \lambda) \leqslant \tfrac{1}{4}a^2(1 + \mu)^2,$$

whereas

$$|y| \leqslant \frac{x_0 y_0 - |x| y_0}{x_0} = y_0 - \tfrac{1}{4}\mu a^2 y_0^2 .$$

Hence

$$\begin{aligned}|(x+t)(y+t)(t-a)| &\leqslant \tfrac{1}{4}(1+\mu)^2(a^2y_0 - \tfrac{1}{4}\mu a^4 y_0^2 + a^3\lambda)\\ &\leqslant \tfrac{1}{4}(1+\mu)^2(a^2y_0 - \tfrac{1}{4}\mu a^4 y_0^2 + \tfrac{1}{2}a^3)\\ &\leqslant \tfrac{1}{4}(1+\mu)^2(a^2y_0 - \tfrac{1}{4}\mu(a^2y_0)^2 + \tfrac{2}{7}).\end{aligned}$$

But $a^2y_0 \leqslant 4\sqrt{\frac{3}{14}}$ and, as a function of z, $z - \frac{1}{4}\mu z^2$ has a maximum at $z = 2/\mu > 4\sqrt{\frac{3}{14}}$. Therefore

$$|(x+t)(y+t)(t-a)| \leqslant \tfrac{1}{4}(1+\mu)^2(4\sqrt{\tfrac{3}{14}} + \tfrac{2}{7} - \tfrac{6}{7}\mu) = h(\mu), \quad \text{say.}$$

Computing, we find that $h'(\mu) \geqslant 0$ if $0 \leqslant \mu \leqslant \frac{1}{2}$ and also $h(\frac{1}{2}) < 1$. This completes Case C.

Case D $\frac{1}{2}a \leqslant x \leqslant \frac{3}{4}a$ Put $x = \mu a$, so that $\frac{1}{2} \leqslant \mu \leqslant \frac{3}{4}$. Assume first that $y < 0$. We shall show that the interval $0 < t < a$ will suffice. To begin

$$(x+t)(a-t) \leqslant \tfrac{1}{4}(a+x)^2.$$

Thus, if $y \geqslant -a$, then

$$|(x+t)(y+t)(t-a)| \leqslant \tfrac{1}{4}a(a+x)^2 \leqslant a^3 < 1.$$

On the other hand, if $y < -a$, then

$$\begin{aligned}|(x+t)(y+t)(t-a)| &\leqslant \tfrac{1}{4}|y|(a+x)^2\\ &\leqslant \tfrac{1}{4}(1+\mu)^2(a^2y_0 - \tfrac{1}{4}\mu(a^2y_0)^2)\\ &\leqslant \tfrac{1}{4}(1+\mu)^2(4\sqrt{\tfrac{3}{14}} - \tfrac{1}{4}\mu(4\sqrt{\tfrac{3}{14}})^2) = i(\mu), \quad \text{say.}\end{aligned}$$

Computing as before, $i'(\mu)$ is positive and so $i(\mu)$ is monotone increasing in $[\frac{1}{2}, \frac{3}{4}]$ and $i(\frac{3}{4}) < 1$, which takes care of $y < 0$. Now assume that $y \geqslant 0$. We show that the interval $(-\frac{1}{4} - \mu)a \leqslant t \leqslant (\frac{3}{4} - \mu)a$ will suffice. Put $t = \lambda a$ so that $-\frac{1}{4} \leqslant \lambda + \mu \leqslant \frac{3}{4}$. Suppose that $0 \leqslant \lambda + \mu \leqslant \frac{3}{4}$. Then with

$$f(t) = |(x+t)(y+t)(t-a)| = (\lambda+\mu)(1-\lambda)|(a^2y + a^3\lambda)|,$$

if $a^2y + a^3\lambda < 0$ it is clear that $f(t) < 1$, so we may assume that $a^2y + a^3\lambda \geqslant 0$ and so

$$\begin{aligned}f(t) &\leqslant (\lambda+\mu)(1-\lambda)(4\sqrt{\tfrac{3}{14}} - \tfrac{6}{7}\mu + a^3(\tfrac{3}{4} - \mu))\\ &\leqslant (\lambda+\mu)(1-\lambda)(4\sqrt{\tfrac{3}{14}} + \tfrac{3}{7} - \tfrac{10}{7}\mu) = j(\mu), \quad \text{say.}\end{aligned}$$

Computing as before, we find that $j'(\mu)$ is positive in the range in question and so the maximum value of $j(\mu)$ occurs when $\lambda + \mu = \frac{3}{4}$. Hence

$$f(t) \leqslant \tfrac{3}{4}(1-\lambda)(4\sqrt{\tfrac{3}{14}} - \tfrac{9}{14} + \tfrac{10}{7}\lambda) = k(\lambda), \quad \text{say.}$$

Further

$$k(\lambda) = \tfrac{3}{4}(1-\lambda)(\alpha + \beta\lambda), \qquad \text{where} \quad \alpha = 4\sqrt{\tfrac{3}{14}} - \tfrac{9}{14} \quad \text{and} \quad \beta = \tfrac{10}{7},$$

has a maximum value of

$$3(\alpha + \beta)^2/16\beta < 1,$$

and so $f(t) < 1$ when $0 \leqslant \lambda + \mu \leqslant \frac{3}{4}$. Now suppose that $-\frac{1}{4} \leqslant \lambda + \mu \leqslant 0$. Then $f(t)$ is not larger than one of the two expressions

$$|(\lambda + \mu)(1 - \lambda)a^2 y| \qquad \text{and} \qquad |(\lambda + \mu)(1 - \lambda)a^3 \lambda|,$$

both of which are less than 1 since $a^2 y \leqslant 4\sqrt{\frac{3}{14}} - \frac{1}{4}\mu(4\sqrt{\frac{3}{14}})^2$ and $|\lambda| < 1$. This clears Case D.

Case E $\frac{3}{4} \leqslant \mu \leqslant 1$ Assume first that $y > 0$. Since $f(t)$ has zeros at a and $-x$ and has no zero between, it follows that either the interval $0 < t < a$ will suffice or $f(t) < 1$ on the interval $-x \leqslant t < 0$. But if $-a \leqslant t \leqslant -x$, then $f(t)$ is not larger than one of the two expressions

$$|(x + t)(a - t)y| \qquad \text{and} \qquad |(x + t)(a - t)a|$$

both of which are less than 1 since $a^2 y < 2$.

Now suppose that $y \leqslant 0$. As in Case D, if $y \geqslant -a$, then the interval $0 < t < a$ will work. Hence we may assume that $y < -a$. Again either the interval $0 < t < a$ suffices or $f(t) < 1$ for $-x \leqslant t < 0$. Thus suppose that $-a < t \leqslant -x \leqslant -\frac{3}{4}a$. Then $|x + t| \leqslant \frac{1}{4}a$, $|a - t| \leqslant 2a$ and so

$$f(t) \leqslant \tfrac{1}{2}(a^2|y| + a^3) \leqslant \tfrac{1}{2}(4\sqrt{\tfrac{3}{14}} - \tfrac{6}{7}\mu + \tfrac{4}{7}) < 1.$$

This completes Case E and we have now covered all the possibilities when $a^3 \geqslant \theta$. Thus, assume from now on that $a^3 \leqslant \theta$.

Case C $0 \leqslant x \leqslant \frac{1}{2}a$ Set $y^* = 2\sqrt{\frac{3}{7}} + 2\sqrt{\frac{3}{7} - s}$ and let $0 \leqslant \mu$, $|\lambda| \leqslant 1$ be constants.

Auxiliary Lemma *If* $\lambda + 2\mu \leqslant \sqrt{\frac{7}{3}}$, *then the maximum value of* $g(s) = y^* - \frac{1}{4}\mu y^{*2} + s\lambda$ *is at* $s = 0$ *in the range* $[0, \frac{3}{7}]$.

Proof $g'(s) = (\frac{3}{7} - s)^{-1/2}(\lambda\sqrt{\frac{3}{7} - s} - 1 + \frac{1}{2}\mu y^*)$. By hypothesis

$$\lambda + \mu \leqslant (1 - \mu\sqrt{\tfrac{3}{7}})(\tfrac{3}{7})^{-1/2} \leqslant (1 - \mu\sqrt{\tfrac{3}{7}})(\tfrac{3}{7} - s)^{-1/2},$$

hence $\lambda(\frac{3}{7} - s)^{1/2} - 1 + \frac{1}{2}\mu y^* \leqslant 0$ and $g'(s) \leqslant 0$. This proves the lemma.

Assume that $0 < t < a$. Then

$$\begin{aligned} f(t) &= |(y_0(x + t)x_0(y + t)(a - t)/x_0 y_0| \\ &\leqslant (\tfrac{1}{4}y_0|x + t| + \tfrac{1}{4}x_0|y + t|)^2|a - t|a \\ &\leqslant (a^{-1} + t\sqrt{\tfrac{3}{7}}a^{-2})^2|a - t|a. \end{aligned}$$

Put $t = \lambda a$ so that $0 < \lambda < 1$ and

$$f(t) \leqslant (1 + \sqrt{\tfrac{3}{7}}\lambda)^2(1 - \lambda) = n(\lambda), \quad \text{say.}$$

Computing in the usual way, we find that $n'(\lambda) \leqslant 0$ if $\lambda \geqslant \frac{1}{3}$. However, $n(1) = 0$ and $n(\frac{1}{3}) = (1 + 21^{-1/2})^2 \frac{2}{3} < 1$. Hence $f(t) < 1$ if $\frac{1}{3} \leqslant \lambda < 1$. So assume $0 < \lambda < \frac{1}{3}$. Since with $x = \mu a$, so $0 \leqslant \mu \leqslant \frac{1}{2}$, it follows that $\lambda + 2\mu \leqslant \frac{4}{3} < \sqrt{\frac{7}{3}}$. Thus the auxiliary lemma applies and

$$\begin{aligned} f(t) &\leqslant (\lambda + \mu)(1 - \lambda)(a^2 |y| + \lambda a^3) \\ &\leqslant (\lambda + \mu)(1 - \lambda)(a^2 y_0 - \tfrac{1}{4}\mu a^4 y_0^2 + \lambda a^3). \end{aligned}$$

Since $a^3 \leqslant \theta$, so $y_0 a^2 \leqslant 2\sqrt{\frac{3}{7}} + 2\sqrt{\frac{3}{7} - a^3} = y^*$. Recalling that $z - \frac{1}{4}\mu z^2$ is monotone increasing for $z \leqslant 2/\mu$ and $2/\mu \geqslant 4 > y^*$, so

$$\begin{aligned} f(t) &\leqslant (\lambda + \mu)(1 - \lambda)(y^* - \tfrac{1}{4}\mu y^{*2} + \lambda a^3) \\ &\leqslant (\lambda + \mu)(1 - \lambda)(4\sqrt{\tfrac{3}{7}} - \tfrac{12}{7}\mu) \qquad \text{by the auxiliary lemma,} \\ &\leqslant \tfrac{1}{4}(1 + \mu)^2(4\sqrt{\tfrac{3}{7}} - \tfrac{12}{7}\mu) \end{aligned}$$

by the arithmetic–geometric mean inequality, $= p(\mu)$ say. The customary computation shows that $p'(\mu) > 0$ since $\mu \leqslant \frac{1}{2}$ and so $p(\mu) \leqslant p(\frac{1}{2}) < 1$. This completes Case C.

Case D $\frac{1}{2}a \leqslant x \leqslant .694a$ Assume first that $y \geqslant 0$. Again put $x = \mu a$ and $t = \lambda a$ so that $\frac{1}{2} \leqslant \mu \leqslant .694$. We show that the interval for t given by $-.306 - \mu \leqslant \lambda \leqslant .694 - \mu$ will suffice. We have

$$f(t) = |(x + t)(y + t)(a - t)| = |(\lambda + \mu)|(1 - \lambda)(a^2 y + a^3 \lambda).$$

Here we may assume that $a^2 y + a^3 \lambda > 0$ for otherwise, since $|\lambda| \leqslant 1$ and $|\lambda + \mu| \leqslant .694$, it follows easily that $f(t) < 1$. Further, with $y^* = 2\sqrt{\frac{3}{7}} + 2\sqrt{\frac{3}{7} - a^3}$, the previous argument applies because $2/\mu \geqslant 2/.694 > 4\sqrt{\frac{3}{7}}$. Therefore

$$f(t) \leqslant |(\lambda + \mu)|(1 - \lambda)(y^* - \tfrac{1}{4}\mu y^{*2} + a^3 \lambda).$$

But $\lambda + 2\mu \leqslant .694 + .694 < \sqrt{\frac{7}{3}}$ and the auxiliary lemma applies. Hence

$$f(t) \leqslant |(\lambda + \mu)|(1 - \lambda)(4\sqrt{\tfrac{3}{7}} - \tfrac{12}{7}\mu).$$

Suppose first that $0 \leqslant \lambda + \mu \leqslant .694$, so that

$$|\lambda + \mu|(1 - \lambda) = (\lambda + \mu)(1 - \lambda)$$

which, as a function of λ has a maximum at $\lambda = \frac{1}{2}(1 - \mu)$. However, λ is always less than this value since

$$2\lambda + \mu \leqslant .694 + (.694 - .5) < 1.$$

Hence we are justified in replacing $\lambda + \mu$ by .694 and so

$$f(t) \leqslant .694(.306 + \mu)(4\sqrt{\tfrac{3}{7}} - \tfrac{12}{7}\mu) = q(\mu), \quad \text{say.}$$

The customary computation of the maximum of $q(\mu)$ yields

$$q(\mu) \leqslant .694(1 + .306\sqrt{\tfrac{3}{7}})^2 = .999899\ldots < 1.$$

Suppose now that $-.306 \leqslant \lambda + \mu \leqslant 0$. Then

$$|\lambda + \mu|(1 - \lambda) = -(\lambda + \mu)(1 - \lambda),$$

and, since $\lambda < 0$, this is a maximum when $\lambda = -.306 - \mu$. Therefore

$$f(t) \leqslant .306(1.306 + \mu)(4\sqrt{\tfrac{3}{7}} - \tfrac{12}{7}\mu) = r(\mu), \quad \text{say.}$$

$r(\mu)$ has its maximum at $\mu = \frac{1}{2}\sqrt{\frac{7}{3}} - .653 < \frac{1}{2}$. Since $\mu \geqslant \frac{1}{2}$ it follows that

$$r(\mu) \leqslant .306(1.806)(4\sqrt{\tfrac{3}{7}} - \tfrac{6}{7}) < 1.$$

Thus the lemma holds in this case if $y \geqslant 0$.

Now assume that $y < 0$. Again we may assume that $y < -a$ for otherwise, taking $0 < t < a$, we have $f(t) \leqslant 2a \cdot a \cdot a < \frac{6}{7} < 1$. Then $f(t)$ has roots $-x$, a, and $-y > a$ and so either $0 < t < a$ will suffice or $f(t) < 1$ on $-x \leqslant t < 0$. Hence we may assume that $f(t) < 1$ on $-\mu \leqslant \lambda < 0$. In addition, if $0 < \lambda \leqslant .694 - \mu$, the argument for $y > 0$ above goes through virtually unchanged since if $a^2y + a^3\lambda$ is positive then an upper bound is $.194a^3$ and $f(t) < 1$, whereas if $a^2y + a^3\lambda$ is nonpositive, then its modulus is bounded above by $a^2|y| \leqslant y^* - \frac{1}{4}\mu y^{*2}$ and the auxiliary lemma may be applied with $\lambda = 0$ yielding the same bound as before. Hence we may assume that $-.306 \leqslant \lambda + \mu \leqslant 0$. It is then evident that, as a function of λ, $f(t)$ is a maximum when $\lambda + \mu = -.306$. Hence, incorporating previous arguments

$$f(t) \leqslant .306(1.306 + \mu)(y^* - \tfrac{1}{4}\mu y^{*2} + a^3(\mu + .306))$$

where $y^* = 2\sqrt{\frac{3}{7}} + 2\sqrt{\frac{3}{7} - a^3}$.

Put $u(a^3) = y^* - \frac{1}{4}\mu y^{*2} + a^3(\mu + .306)$ and, for simplicity of notation, $\alpha = \sqrt{\frac{3}{7}}$ and $\beta = .306$. Then $u(a^3)$, considered as a function of a^3, attains its maximum at

$$a^3 = \alpha^2 - \left(\frac{1 - \mu\alpha}{2\mu + \beta}\right)^2$$

and with this value of a^3, after a little more computation,

$$y^* - \tfrac{1}{4}\mu y^{*2} + a^3(\mu + .306) = (\mu\alpha + \alpha\beta + 1)^2/(2\mu + \beta).$$

Hence

$$f(t) \leqslant \beta(1 + \beta + \mu)(\mu\alpha + \alpha\beta + 1)^2/(2\mu + \beta) = v(\mu)$$

say. Now $v'(\mu)$ has the same sign as

$$(\mu\alpha + \alpha\beta + 1 + 2\alpha(1 + \beta + \mu))(2\mu + \beta) - 2(1 + \beta + \mu)(\mu\alpha + \alpha\beta + 1)$$

which is a quadratic in μ with leading coefficient $4\alpha > 0$. Further, at $\mu = 0$ its

value is $\alpha\beta^2 - \beta - 2 < 0$ since $\alpha = \sqrt{\frac{3}{7}}$ and $\beta = .306$. It follows that the maximum value of $v(\mu)$ on $\frac{1}{2} \leqslant \mu \leqslant .694$ is

$$\max(v(\tfrac{1}{2}), v(.694)) = \max(.987\ldots, .989\ldots) < 1.$$

This completes Case D.

Case E $.694a \leqslant x \leqslant a$ Assume first that $y > 0$. We show that the interval $-a < t < 0$ will suffice. If $0 < y \leqslant a$ and $-a < t < 0$, it is trivial that $f(t) < 1$. Thus we assume that $y > a$. As before, $f(t)$ has roots $-x$, a, and $-y < -a \leqslant -x$ and so either $f(t) < 1$ on $0 < t < a$ or $f(t) < 1$ on $-x \leqslant t < 0$. Thus we need to show only that $f(t) < 1$ on $-a < t \leqslant -x$. Again put $t = \lambda a$ and $x = \mu a$ so that $-1 < \lambda \leqslant -\mu$, and $.694 \leqslant \mu \leqslant 1$. Now

$$f(t) = |\lambda + \mu|(a^2 y + a^3\lambda)(1 - \lambda).$$

But $a^2 y + a^3\lambda \leqslant a^2 y \leqslant a^2 y_0 - \frac{1}{4}(a^2 y_0)^2 \leqslant 1/\mu$, the maximum value in z of $z - \frac{1}{4}\mu z^2$, $\leqslant 1/.694$. Hence

$$f(t) \leqslant .306(2)(1/.694) < 1.$$

Therefore we may assume from now on that $y \leqslant 0$. Exactly as before we may assume that $y < -a$ so that either $f(t) < 1$ on $0 < t < a$ or $f(t) < 1$ or $-x \leqslant t < 0$. Hence it remains to show that $f(t) < 1$ on $-a < t \leqslant -x$, i.e., on $-1 < \lambda \leqslant -\mu$. In this case

$$f(t) \leqslant 2(1 - \mu)(a^2|y| + a^3) \leqslant 2(1 - \mu)(a^2 y_0 - \tfrac{1}{4}\mu(a^2 y_0)^2 + a^3).$$

Suppose first that $.694 \leqslant \mu \leqslant .76$. Since

$$2/\mu \geqslant 2/.76 > 4\sqrt{\tfrac{3}{7}},$$

so $f(t) \leqslant 2(1 - \mu)(y^* - \frac{1}{4}\mu y^{*2} + a^3)$ and clearly this is greatest when μ is least, namely .694. However, the case $\lambda = -1$, $\mu = .694$, $y < 0$ has already been considered, and we have shown here that $f(t) \leqslant 1$. Hence it remains to consider the possibility that $.76 \leqslant \mu \leqslant 1$. Let $-a < t \leqslant 0$. Arguing as before, it is sufficient to consider $-a < t \leqslant -x$, i.e., $-1 < \lambda \leqslant -\mu$ and then

$$\begin{aligned} f(t) &\leqslant |\lambda + \mu|\,|1 - \lambda|(a^2|y| - a^3\lambda) \\ &\leqslant |\lambda + \mu|\,|1 - \lambda|\left(\frac{1}{\mu} + a^3\right) \leqslant (.24)(2)\left(\frac{1}{.76} + \frac{3}{7}\right) < 1, \end{aligned}$$

and this completes the proof of Lemma 2.

REFERENCES

[1] B. J. Birch and H. P. F. Swinnerton-Dyer, On the inhomogeneous minimum of the product of n linear forms, *Mathematika* **3** (1956), 25–39.

[2] A. J. Cole, On the product of n linear forms, *Quart. J. Math. Oxford Ser.* **3** (1952), 56–62.
[3] H. Davenport, Note on the product of three homogeneous linear forms, *J. London Math. Soc.* **16** (1941), 98–101.
[4] B. F. Skubenko, On Minkowski's conjecture for $n = 5$, *Soviet Math. Dokl.* **13** (1972), 1136–1138 [translation of *Doklady Akad. Nauk SSSR* **205** (1972), 1304–1305 (Russian)].

On the Degrees of the Sum and Product of Two Algebraic Elements

BOHUSLAV DIVIŠ†

THE OHIO STATE UNIVERSITY
COLUMBUS, OHIO

If $\alpha + \beta$ is not a generator of the composite field $K(\alpha, \beta)$, where $K(\alpha)$ and $K(\beta)$ are linearly disjoint separable algebraic extensions of the field K of degrees m and n, then char K *is a divisor of mn or it is smaller than $\frac{1}{2}\min(m, n)$. If $\alpha\beta$ does not generate $K(\alpha, \beta)$, then both fields $K(\alpha)$ and $K(\beta)$ are, essentially, radical extensions of K.*

Let K be a field and let $K(x)$ and $K(y)$ be simple separable algebraic extensions of K of finite degrees m and n, say, such that $[K(x, y):K] = mn$. The composite field $K(x, y)$ is also a simple extension of K, and experience tells us that it is usually generated by $x + y$. This has been confirmed by Isaacs [1] for char $K = 0$, or char $K = p \nmid mn$ and $p > \min(m, n)$. Another proof of a weaker result in a more general context has recently been given in [2].

The purpose of this article is twofold. Firstly, we shall show that $K(x, y) = K(x + y)$ already if $p \nmid mn$ and $p > \frac{1}{2}\min(m, n)$. Secondly, we shall study the analogous question for the products and give a complete description of the extensions in which xy does not generate $K(x, y)$. They turn out to be, essentially, radical extensions.

† Deceased.

Let us assume that $[K(x, y):K(x + y)] = k > 1$. The five fields K, $(K(x)$, $K(y)$, $K(x + y)$, and $K(x, y)$ will be said to form a *deficient system* (with deficiency k). Let us denote by $x = x_1, x_2, \ldots, x_m$ and $y = y_1, y_2, \ldots, y_n$ the conjugates of x and y. Let us denote by $\bar{K}_x$, $\bar{K}_y$, and $\bar{K}_{x,y}$ the normal closures of $K(x)$, $K(y)$, and $K(x, y)$ over K.

By our assumption, all the Galois groups $\mathrm{Gal}(\bar{K}_y(x_i)/K(x_i))$ $(1 \le i \le m)$ are transitive on the y's and the groups $\mathrm{Gal}(\bar{K}_x(y_j)/K(y_j))$ $(1 \le j \le n)$ are transitive in the x's. Therefore, $\mathrm{Gal}(\bar{K}_{x,y}/K)$ acts transitively on the sums $x_i + y_j$ $(1 \le i \le m, 1 \le j \le n)$. Since we assume that $\deg(x + y) = mn/k$, we must have a system of mn/k equations of the type

$$x_{i_1} + y_{j_1} = x_{i_2} + y_{j_2} = \cdots = x_{i_k} + y_{j_k}, \tag{1}$$

where the sums of $x_i + y_j$ in different equations are distinct and the group $\mathrm{Gal}(\bar{K}_{x,y}/K)$ acts on the equations transitively.

Two equations of the type (1) will be called *directly linked* (with respect to x) if there is x_i that appears in both of them. Two such equations will be called *linked* (with respect to x) if there is a chain of directly linked equations connecting them. Contrary to direct linkage, the concept of linkage is an equivalence relation and our equations will be partitioned in equivalence classes. An equivalence class containing x_i, say, in one of the equations will contain all equations containing x_i. Therefore, the class that contains $x = x_1$ will contain all equations in which occur some of the conjugates $x_1, x_2, \ldots, x_{m_1}$, say. By the transitivity of $\mathrm{Gal}(\bar{K}_{x,y}/K)$ on the equivalence classes, all classes will likewise contain m_1 conjugates of x, and thus $m_1 \mid m$. Every transformation from $\mathrm{Gal}(\bar{K}_{x,y}/K)$ that carries over x_i $(1 \le i \le m_1)$ into x_j $(1 \le j \le m_1)$ fixes the whole equivalence class containing x_1 and thus it permutes the elements $x_1, x_2, \ldots, x_{m_1}$ and fixes the field

$$K' = K\left(\sum_{i=1}^{m_1} x_i; \sum_{1 \le i < j \le m_1} x_i x_j; \ldots; x_1 x_2 \cdots x_{m_1}\right).$$

Therefore, $K' \subset K(x)$ and the elements $x_1, x_2, \ldots, x_{m_1}$ are conjugate with respect to K' and their degree is $m_1 \mid m$. Furthermore, we have $K(x) = K'(x)$, $K(x, y) = K'(x, y)$, and $K(y) \subset K'(y) \subset K'(x, y)$. It follows that

$$[K'(x, y):K'(y)] = [K'(x):K'] = m_1$$

and

$$[K'(x, y):K'(x)] = [K'(y):K'] = n.$$

Moreover, $[K'(x, y):K(x + y)] = k$ since the equations (1) are unchanged.

In this way we have obtained the same situation over the ground field K' as we had over K, namely the deficiency k by which the degree of $x + y$ has to be divided is unchanged. Now we shall perform the same kind of reduc-

tion over K' with respect to y. If it happens that we destroy the linkage with respect to x, we shall perform the reduction with respect to x again, and if necessary, once more with respect to y, etc. After finitely many steps, we shall have a ground field $K^* \subset K(x, y)$ such that

$$[K^*(x, y):K^*(x)] = [K^*(y):K^*] = n^* \mid m,$$

$$[K^*(x, y):K^*(y)] = [K^*(x):K^*] = m^* \mid m,$$

$$[K^*(x, y):K^*(x + y)] = k > 1, \qquad \text{and all equations (1)}$$

for the sums $x_i + y_j$ $(1 \leq i \leq m^*, 1 \leq j \leq n^*)$ will be linked both with respect to x and y. The five fields K^*, $K^*(x)$, $K^*(y)$, $K^*(x + y)$, and $K^*(x, y)$ will be said to form a *primitive deficient system* (with parameters p, m^*, n^*, and k). In the following we shall restrict ourselves to primitive systems only.

Remark If K, $K(x)$, $K(y)$, $K(x + y)$, and $K(x, y)$ form a primitive system, there still can be a nontrivial subfield between K and $K(x)$ or $K(y)$.

Theorem 1 *Let K, $K(x)$, $K(y)$, $K(x + y)$, and $K(x, y)$ form a primitive system with parameters $p = \operatorname{char} K$, $m = [K(x):K]$, $n = [K(y):K]$, and $k = [K(x, y):K(x + y)] > 1$. If $p \nmid mn/k$, then $\bar{K}_x = \bar{K}_y = \bar{K}_{x,y}$, and if $p \nmid m$, then $\bar{K}_x \subseteq \bar{K}_y$, i.e., $m \mid (n - 1)!$.*

Theorem 2 *If K, $K(x)$, $K(y)$, $K(x + y)$, and $K(x, y)$ form a primitive system of characteristic p, then $p \mid [\bar{K}_{x,y}:K]$.*

Proof of Theorem 1 Primitive systems have one important property, namely every x_i $(1 \leq i \leq m)$ can be written in the form

$$x_i = x_1 + \sum_{j=1}^{n} \lambda_{ji} y_j, \qquad \sum_{j=1}^{n} \lambda_{ji} = 0 \qquad (1 \leq i \leq m) \tag{2}$$

and every y_j $(1 \leq j \leq n)$ can be written as

$$y_j = y_1 + \sum_{i=1}^{m} \mu_{ij} x_i, \qquad \sum_{i=1}^{m} \mu_{ij} = 0 \qquad (1 \leq j \leq n) \tag{3}$$

where the λ's and μ's are rational integers. This is a consequence of the two-sided linkage. Note that the representations (2) and (3) may not be unique. Using (2) we see that

$$\operatorname{tr}(x + y) = (mn/k)x_1 + Y,$$

when $Y \in \bar{K}_y$. If $p \nmid mn/k$, then it follows that $x_1 \in \bar{K}_y$ and this implies $\bar{K}_x \subseteq \bar{K}_y$. If we use Eqs. (3), we similarly obtain $\bar{K}_y \subseteq \bar{K}_x$. If $p \nmid m$, then (2) implies $\operatorname{tr} x = mx_1 + Y$, $Y \in \bar{K}_y$, and that yields $x_1 \in \bar{K}_y$, which in turn implies $\bar{K}_x \subseteq \bar{K}_y$.

Proof of Theorem 2 Without loss of generality we may assume that

$p \nmid mn$, and hence we may assume that tr $x = $ tr $y = 0$. By (2), we have

$$x_1 = \sum_{j=1}^{n} v_j y_j, \qquad \sum_{j=1}^{n} v_j = 0, \qquad v_j \in K \qquad (1 \leq j \leq n). \tag{4}$$

For every $\varphi \in G = \mathrm{Gal}(\bar{K}_y(x_1)/K(x_1))$ is

$$x_1 = \sum_{j=1}^{n} v_j \varphi(y_j).$$

If we add up all these equations, we obtain

$$[K_y(x_1):K(x_1)] \cdot x_1 = \sum_{\varphi \in G} \sum_{j=1}^{n} v_j \varphi(y_j) = \sum_{j=1}^{n} v_j \sum_{\varphi \in G} \varphi(y_j) = \sum_{j=1}^{n} v_j \text{ tr } y = 0.$$

This implies

$$p \mid [\bar{K}_y(x_1):K(x_1)] \mid [\bar{K}_{x,y}:K].$$

Theorem 3 *The condition $p \mid [\bar{K}_{x,y}:K]$ must be satisfied in every deficient system. If $m \geq n$ and $p > n$, then $p \mid m$. In particular, $p \leq \max(m, n)$.*

Proof The condition $p \mid [\bar{K}_{x,y}:K]$ is a consequence of Theorem 2 and of the "divisibility preserving" property of every reduction procedure to a primitive system. The second statement also holds for primitive systems. Namely, in the proof of Theorem 2 we found that $p \nmid mn$ implies $p \mid [\bar{K}_y(x_1):K(x_1)]$, and Theorem 1 says that $\bar{K}_y(x_1) = \bar{K}_y$ if $p \nmid mm$. Therefore, we must have $p \mid [\bar{K}_y:K] \mid n!$, which is tantamount to $p \leq n$, and as a consequence of the divisibility preserving property of every reduction procedure, it holds for every deficient system.

Theorem 4 *If one of the parameters m or n of a deficient system is a prime power, then $p \mid mn$.*

Proof It suffices to consider primitive systems only. If $n = q^\beta$ and $p \nmid mn$, then we have Eq. (4) as in the proof of Theorem 2. As a next step, however, we shall not apply the full group $G = \mathrm{Gal}(\bar{K}_y(x_1)/K(x_1))$ to it but merely its Sylow q-subgroup G_q, say. It is well known that G_q is transitive on the y's and therefore does not depend on j. It follows that

$$|G_q| \cdot x_1 = \sum_{\varphi \in G_q} \sum_{j=1}^{n} v_j \varphi(y_j) = \sum_{j=1}^{n} v_j \sum_{\varphi \in G_q} \varphi(y_j) = 0,$$

which is a contradiction.

Theorems 1–4 have been first proved by Isaacs [1]. The proofs given here are not essentially different, but they seem to be using simpler language. Also, they differ in the concept of a primitive system.

Now we would like to propose the following

Problem Describe all primitive deficient systems.

In this connection, it seems to be reasonable to introduce the following definition. A primitive deficient system will be called *regular* if $k = n \leq m$, and *irregular* otherwise.

Theorem 5 *In a regular primitive deficient system with* $k = n \leq m$ *is necessarily* $m = p^\alpha$, *where* $1 \leq \alpha \leq n - 1$.

Proof We have $[K(x_1 + y_1):K] = m$ and $K(x_1 + y_1, y_1) = K(x_1, y_1)$, and therefore the fields $K(x_1 + y_1)$ and $K(y_1)$ are linearly disjoint. If we have $x_1 + y_1 = x_2 + y_2$, say, we have $x_2 = x_1 + y_1 - y_2$. We can fix y_2 and send $x_1 + y_1$ to an arbitrary sum $x_i + y_j$ and then fix $x_i + y_j$ and send y_2 to an arbitrary y_l. This shows that every expression $x_i + y_j - y_l$ is among the conjugates of x_1. It follows that every expression

$$x_1 + \sum_{j=1}^{n} \lambda_j y_j \qquad \left(\sum_{j=1}^{n} \lambda_j = 0, \quad 0 \leq \lambda_j \leq p - 1 \right)$$

is a conjugate of x_1. Conversely, by (2) every x_i can be written in such a way. If we denote by α the number of linearly independent conjugates of y_1, then $m = p^\alpha$ (elements $y_1, y_2, \ldots, y_r$ are called linearly independent if $\sum_{j=1}^{r} \lambda_j y_j \in K$, $\lambda_j \in \mathbb{Z}_p \Rightarrow \lambda_1 = \lambda_2 = \cdots = \lambda_r = 0$).

The primitive systems can be described by the equations (1) satisfied by the conjugates $x_i + y_j$. Two systems will be considered the same if the equations differ by a permutation of the conjugates $x_1, x_2, \ldots, x_m$ and $y_1, y_2, \ldots, y_n$ only. By abuse of language we shall refer to these systems of equations as to the primitive systems, regardless of their algebraic representation. We shall write for brevity $i\,j = k\,l$ instead of $x_i + y_j = x_k + y_l$.

If $2 = n \leq m$, then $k = 2$, and thus $m = p$ by Theorem 5. We have one regular primitive system for every p with equations

$$1\,1 = 2\,2$$
$$2\,1 = 3\,2$$
$$\vdots$$
$$p\,1 = 1\,2.$$

If $3 = k = n \leq m$, then $m = p^2$ or p. For every p, we have one regular system with $m = p^2$. The equations can easily be written down. For $p = 3$ and for every $p \equiv 1$ (3) there is one regular system with $m = p$. Let us remark that for $p = 3$ is $\operatorname{tr} y = 0$ if $m = 3$, and $\operatorname{tr} y \neq 0$ if $m = 3^2$.

If $4 = k = n \leq m$, then $m = p^3$, p^2, or p. For every p, there is one regular system with $m = p^3$. If $m = p^2$, there is one regular system for $p = 2$ and

$p \equiv -1$ (4) and two regular systems for $p \equiv 1$ (4). Namely, for every p there is the possibility $y_1 + y_2 = y_3 + y_4 = 0$, and for $p \equiv 1$ (4) we also may have $y_3 = \lambda y_1 + (\lambda - 1)y_2$, where $\lambda^2 = -1$. If $p \equiv 1$ (4), then there is also one regular system with $m = p$.

Of particular interest are the irregular systems. There is just one such system for $3 = n \leq m$, with $k = 2$, $m = 6$, and $p = 3$. The equations are

$$1\,1 = 2\,2 \qquad 4\,1 = 5\,3 \qquad 1\,2 = 4\,3$$
$$2\,1 = 3\,3 \qquad 5\,1 = 6\,2 \qquad 3\,2 = 6\,3$$
$$3\,1 = 4\,2 \qquad 6\,1 = 1\,3 \qquad 5\,2 = 2\,3.$$

For $4 = n \leq m$, there is also just one irregular system, with $k = 3$, $m = 6$, and $p = 2$. The equations are

$$1\,1 = 2\,2 = 3\,3 \qquad 4\,1 = 2\,4 = 6\,3$$
$$2\,1 = 1\,2 = 4\,4 \qquad 4\,2 = 1\,4 = 5\,3$$
$$3\,1 = 1\,3 = 5\,4 \qquad 3\,4 = 5\,1 = 6\,2$$
$$3\,2 = 2\,3 = 6\,4 \qquad 4\,3 = 5\,2 = 6\,1.$$

Although the proofs of the last statements are rather tedious, they are not difficult in principle and will be omitted here.

From these examples it might seem that mn/k is always a p-power. However, this is not the case. Namely, for $n = 6$, $m = 10$, $k = 4$, and $p = 2$ ($mn/k = 15$) we have the irregular system

$$1\,1 = 2\,2 = 3\,3 = 4\,4 \quad 1\,6 = 6\,2 = 8\,3 = 10\,4 \quad 3\,4 = 4\,3 = 5\,6 = 6\,5$$
$$1\,2 = 2\,1 = 5\,5 = 6\,6 \quad 2\,3 = 3\,2 = 9\,6 = 10\,5 \quad 3\,5 = 6\,4 = 7\,1 = 10\,2$$
$$1\,3 = 3\,1 = 7\,5 = 8\,6 \quad 2\,4 = 4\,2 = 7\,6 = 8\,5 \quad 3\,6 = 5\,4 = 8\,1 = 9\,2$$
$$1\,4 = 4\,1 = 9\,5 = 10\,6 \quad 2\,5 = 5\,1 = 8\,4 = 10\,3 \quad 4\,5 = 6\,3 = 8\,2 = 9\,1$$
$$1\,5 = 5\,2 = 7\,3 = 9\,4 \quad 2\,6 = 6\,1 = 7\,4 = 9\,3 \quad 4\,6 = 5\,3 = 7\,2 = 10\,1.$$

Although we could construct infinitely many of such examples, namely

$$m = 2^{2t+1} + 2^t, \qquad n = 2^{2t+1} - 2^t, \qquad k = 2^{2t}, \qquad p = 2,$$

$$\frac{mn}{k} = 2^{2t+2} - 1, \qquad t = 1, 2, 3, \ldots,$$

we were as yet unable to construct a system with $p \nmid mn$. However, we can prove the following strengthening of Theorem 3.

Theorem 6 *If $m \geq n$ and $p \nmid mn$ in a deficient system, then $p < \frac{1}{2}n$.*

Proof Let us suppose that $\frac{1}{2}n < p < n$. By Theorem 3, p must divide the order of the group $\mathrm{Gal}(\bar{K}_y(x)/K(x))$ and therefore the group must be primitive on the y's. Since it contains a p-cycle, the group must be $(n - p + 1)$-transitive. If we have $x_1 + y_1 = x_2 + y_2$, say, then there exists a transformation that keeps x_1 and y_1 fixed and sends y_2 to an arbitrary y_j $(j \neq 1)$. Therefore $k = n$ in contradiction to Theorem 5.

Corollary *If $p \nmid mn$ in a deficient system, then* $\min(m, n) \geq 10$.

Proof This follows from Theorems 4 and 6.

Now, let us study the products xy instead of the sums $x + y$. A first information can be obtained from [2]. As a matter of fact, the following theorem is contained in [2] although it is not explicitly stated there.

Theorem 7 *Let K be a field, $0 \notin X \subset K$, $0 \notin Y \subset K$, $|X| = m$, and $|Y| = n$. If there is no element $z \in K$ represented uniquely as $z = xy$, $x \in X$, and $y \in Y$, then there are two natural numbers e and f and two pairs of distinct elements $x_1, x_2 \in X$ and $y_1, y_2 \in Y$ such that*

$$x_1^e = x_2^e \qquad \text{and} \qquad e \leq \min(2^{m+n-2}, n^{m-1})$$

and

$$y_1^f = y_2^f \qquad \text{and} \qquad f \leq \min(2^{m+n-2}, m^{n-1}).$$

The definitions of multiplicative deficient and primitive deficient systems would be analogous. We can prove

Theorem 8 *Let K, $K(x)$, $K(y)$, $K(xy)$, and $K(x, y)$ form a primitive (multiplicative) systems with $[\bar{K}_{x,y}:K] = g$. Then $x^g \in K$ and $y^g \in K$.*

Proof Instead of Eqs. (2), we have

$$x_i = x_1 \prod_{j=1}^{n} y_j^{\lambda_{ji}}, \qquad \sum_{j=1}^{n} \lambda_{ji} = 0 \qquad (1 \leq i \leq m). \tag{5}$$

If we choose one such equation for every i and multiply them out, we obtain

$$N(x) = x_1^m \prod_{j=1}^{n} y_j^{\lambda_j}, \qquad \sum_{j=1}^{n} \lambda_j = 0.$$

If we apply all $\varphi \in G = \mathrm{Gal}(\bar{K}_y(x_1)/K(x_1))$ to it and multiply the resulting equations, we get

$$(N(x))^{g/m} = x_1^g \prod_{j=1}^{n} \left(\prod_{\varphi \in G} \varphi(y_j) \right)^{\lambda_j} = x_1^g$$

since $\bar{K}_y(x_1) = \bar{K}_{x,y}$ by (5), $\prod_{\varphi \in G} \varphi(y_j)$ does not depend on j and $\sum_{j=1}^{n} \lambda_j = 0$. The proof of $y^g \in K$ is analogous.

Let us remark that Theorem 6 does not hold in an arbitrary multiplicative deficient system.

As in the additive case, we can define the regular primitive multiplicative systems by the condition $1 < k = n \leq m$. Let us prove

Theorem 9 *In a regular primitive multiplicative system we have $x^m \in K$ and $y^m \in K$.*

Proof The conjugates of x and y satisfy a system of m equations of the type

$$x_{i_1} y_1 = x_{i_2} y_2 = \cdots = x_{i_n} y_n .$$

If we multiply all of them combining terms containing the same y's, we obtain

$$N(x) y_1^m = N(x) y_2^m = \cdots = N(x) y_n^m,$$

which implies $y_1^m = y_2^m = \cdots = y_n^m \in K$. Instead of Eqs. (2) we have Eqs. (5). If we raise them to the mth power, we get

$$x_i^m = x_1^m, \qquad 1 \leq i \leq m,$$

thus $x^m \in K$.

In difference to the additive case, we can prove

Theorem 10 *All primitive multiplicative systems are regular.*

Proof Let us assume that we have a primitive multiplicative system that is not regular. We can easily see that $x^m \in K$ would imply the regularity of the system. Let $m_1 > m$ be the minimal positive exponent such that $x^{m_1} \in K$ and $y^{m_1} \in K$. We may assume that we have a system with a minimal value of m and then also with a minimal value of m_1. By Theorem 8, m_1 is not divisible by primes larger than m. Let $p \leq m$ be such that $p \mid m_1$. Let us put $X_i = x_i^p$, $Y_j = y_j^p$ for $1 \leq i \leq m$ and $1 \leq j \leq n$. The expressions X_i cannot be all equal since otherwise $x^p \in K$. Therefore, $K(X_i)$ is a nontrivial extension of K of degree at most m. Since the equations for x_i and y_j are linked, the five fields K, $K(X_1)$, $K(Y_1)$, $K(X_1 Y_1)$, $K(X_1, Y_1)$ form a multiplicative deficient system. Finally, $X_i^{m_1/p} \in K$. Thus, the parameters of this new deficient system are certainly smaller than the parameters of the old system. Therefore, this new system must be regular.

Conversely, let us start with this new regular system and put $x^p = X$. This would force the old system to be imprimitive, which is a contradiction.

REFERENCES

[1] J. M. Isaacs, Degrees of sums in a separable field extension, *Proc. Amer. Math. Soc.* **25** (1970), 638–641.

[2] J. Browkin, B. Diviš, and A. Schinzel, Addition of sequences in general fields, *Monatshefte für Mathematik* (to appear).

AMS (MOS) 1970 subject classifications: 12F05, 12F10.

Indices in Cyclic Cubic Fields

D. S. DUMMIT†

PRINCETON UNIVERSITY
PRINCETON, NEW JERSEY

H. KISILEVSKY‡

CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA

If K is an algebraic number field and O_K the algebraic integers in K, let $\mathrm{Ind}(\alpha) = [O_K\colon Z[\alpha]]$ *for* $\alpha \in O_K$. *If* $m(K) = \min_{\alpha \in O_K} \mathrm{Ind}(\alpha)$, *it is shown that $m(K)$ is unbounded as K runs through cubic subfields of the cyclotomic fields of lth roots of unity for l prime and that there exist infinitely many cyclic cubic fields K with $m(K) = l$. We also compute $m(K)$ for some specific examples.*

Let K be an algebraic number field and let O_K be its ring of integers. Given $\alpha \in O_K$, define the "index" of α, written $\mathrm{Ind}(\alpha)$, to be the group index $[O_K\colon Z[\alpha]]$. This index is finite if α generates K over the rationals Q, and α is said to generate a "power basis" if this index is 1, i.e., $O_K = Z[\alpha]$. If $\omega_1 = 1$, $\omega_2, \ldots, \omega_n$ is an integral basis for O_K, then the index of α is the absolute value of the determinant of the matrix transforming the basis $\omega_1, \ldots, \omega_n$ to $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. If $\delta(\alpha) = \prod_{\sigma_i \neq 1} (\alpha - \sigma_i(\alpha))$ (where the product is taken over all nontrivial isomorphisms of K into an algebraic closure), then $\mathrm{Norm}_{K/Q}(\delta(\alpha)) = D(1, \alpha, \ldots, \alpha^{n-1})$ where $D(\alpha_1, \ldots, \alpha_n)$ is the discriminant of $\{\alpha_1, \ldots, \alpha_n\}$. Hence

$$\mathrm{Norm}_{K/Q}(\delta(\alpha)) = \mathrm{Ind}(\alpha)^2 \cdot D(\omega_1, \ldots, \omega_n) = \mathrm{Ind}(\alpha)^2 \cdot D(K),$$

† Supported in part by NSF Grant GY-10621.
‡ Supported in part by NSF Grant GP-40871.

where $D(K)$ is the discriminant of K. Let

$$\alpha = x_1 \cdot 1 + x_2 \cdot \omega_2 + \cdots + x_n \cdot \omega_n .$$

Since $\mathrm{Ind}(\alpha) = \mathrm{Ind}(\alpha - x_1)$, we may assume $x_1 = 0$. Then

$$\alpha^i = f_{i1} \cdot 1 + \cdots + f_{in} \cdot \omega_n$$

where the f_{ij} are forms of degree i in $x_2, \ldots, x_n$. Hence the determinant of the transformation matrix is a form of degree $\frac{1}{2}n(n-1)$ in the $n-1$ variables $x_2, \ldots, x_n$. This form is called the "indicial form," and we shall denote by $m(K)$ the minimal value assumed by the form as α ranges over the integers of K. O_K has a power basis if and only if $m(K) = \pm 1$.

The question of the existence of a power basis was originally examined by Dedekind [4]. It was demonstrated that the ring of integers in the cubic field generated by a root of $x^3 + x^2 - 2x + 8$ has no power basis. The Dedekind example led to the following result of Hensel [11]:

Proposition *The index of every element $\alpha \in O_K$ is divisible by the prime p if and only if*

$$g(f) > \frac{1}{f} \sum_{d|f} \mu\left(\frac{f}{d}\right) p^d$$

for some integer $f \geq 1$, where $g(f)$ denotes the number of prime ideals dividing (p) in K with residue class degree f (such primes are called "common index divisors").

We shall call the case $[K : Q] = 3$ of this result the Dedekind test. We shall be concerned with determining the minimal index for cubic subfields of prime cyclotomic fields.

The cyclotomic field of lth roots of unity K_l contains a (unique) cubic subfield K if and only if $l \equiv 1 \pmod 3$. Let l be such a prime, and ζ any nontrivial solution of $x^l = 1$. Then $K_l = Q(\zeta)$ and the galois group $g(K_l/Q)$ is cyclic of order $l-1$, generated by the automorphism $\tau\colon \zeta \to \zeta^g$, where g is a primitive root mod l. The cubic subfield K is then the fixed field of the subgroup $\langle \tau^3 \rangle$.

If we denote by α the relative trace from K_l to K of ζ, then α is a generator of the field K, $K = Q(\alpha)$. This follows from the fact that α is fixed by $\langle \tau^3 \rangle$ and cannot be rational since fewer than $l-1$ of the elements $\zeta, \zeta^2, \ldots, \zeta^{l-1}$ are linearly independent.

Proposition 1 *The element $\alpha = \mathrm{Tr}_{K_l/K}(\zeta)$ forms a normal basis for O_K, i.e., the elements $\alpha, \sigma(\alpha), \sigma^2(\alpha)$ (the K-conjugates of α) are an integral basis for O_K.*

Proof It suffices to show that each $\gamma \in O_K$ can be written in the form $\gamma = a\alpha + b\sigma(\alpha) + c\sigma^2(\alpha)$ with $a, b, c \in Z$. Since α generates K, $\gamma \in O_K$ implies

$\gamma = r\alpha + s\sigma(\alpha) + t\sigma^2(\alpha)$ where $r, s, t \in Q$. As also $\gamma \in O_{K_l}$, considering this expression in K_l and noting $O_{K_l} = Z[\zeta]$ shows $r, s, t \in Z$.

To determine the arithmetic of the field K, it is convenient to find the minimal polynomial satisfied by α. The solution to this problem is afforded by the theory of cyclotomy.

Proposition 2 *Let l be a prime $\equiv 1 \pmod 3$. Then $4l$ has the (unique) representation $4l = c^2 + 27d^2$, with $c \equiv 1 \pmod 3$, $d > 0$. With respect to this representation, the minimal polynomial for $\alpha = \mathrm{Tr}_{k_l/Q}(\zeta)$ is*

$$f_\alpha(x) = x^3 + x^2 - \left(\frac{l-1}{3}\right)x - \left(\frac{lc + 3l - 1}{27}\right).$$

Proof The number α is a "cyclotomic period" of degree $e = 3$ (i.e., $\alpha = \sum \sigma_i(\zeta)$, $\sigma_i \in \langle \tau^3 \rangle$). The period equation satisfied by α is [5, p. 393]

$$\begin{vmatrix} 1+\alpha & 1 & 1 \\ (1,0)\alpha & (1,1)-\alpha & (1,2) \\ (2,0)\alpha & (2,1) & (2,2)-\alpha \end{vmatrix} = 0$$

where the (i, j) are the "cyclotomic numbers" associated with $e = 3$. These numbers can be computed in terms of l, c, and d, where $4l = c^2 + 27d^2$, $c \equiv 1 \pmod 3$. From Storer [14],

$$18(1,0) = 2l - 4 - c - 9d$$
$$18(1,1) = 2l - 4 - c + 9d$$
$$9(1,2) = l + c + 1$$
$$(2,0) = (1,1),\ (2,1) = (1,2),\ (2,2) = (1,0).$$

Solving the determinant with these values yields the polynomial $f_\alpha(x)$.

The polynomial $f_\alpha(x)$ determines the splitting of all primes in K. The prime l ramifies. Since discriminant $f_\alpha(x) = l^2d^2$ (an elementary calculation), the splitting of all primes $p \nmid d$ is determined by the splitting of $f_\alpha(x)$ in Z/pZ [12, pp. 27–29]. If now $p \mid d$, then $l^2d^2 \equiv 0 \pmod p$, hence $f_\alpha(x)$ splits completely mod p. Thus $\bar{\alpha}, \overline{\sigma(\alpha)}, \overline{\sigma^2(\alpha)} \in Z/pZ$. But since $\alpha, \sigma(\alpha), \sigma^2(\alpha)$ generate O_K over Z, $\bar{\alpha}, \overline{\sigma(\alpha)}, \overline{\sigma^2(\alpha)}$ generate $O_K/\mathfrak{p}$ over Z/pZ ($\mathfrak{p}$ a prime lying above p). Hence $f(\mathfrak{p}/(p)) = 1$, and p splits (completely) in K. Thus the splitting of all primes is determined by f_α.

The theory of cyclotomy also allows ready computation of the indicial form. Using the integral basis $1, \alpha, \sigma(\alpha)$, and using the relations among the periods in Dickson [5, p. 393], we have

$$\beta = x\alpha + y\sigma(\alpha)$$
$$\beta^2 = f_{21} \cdot 1 + f_{22} \cdot \alpha + f_{23} \cdot \sigma(\alpha) = A\alpha + B\sigma(\alpha) + C\sigma^2(\alpha)$$

where

$$A = (0, 0)x^2 + (0, 2)y^2 + 2(0, 1)xy - (p - 1)$$
$$B = (0, 1)x^2 + (0, 0)y^2 + 2(0, 2)xy - (p - 1)$$
$$C = (0, 2)x^2 + (0, 1)y^2 + 2(0, 0)xy - (p - 1).$$

Thus

$$\mathrm{Ind}(\beta) = \pm \begin{vmatrix} 1 & 0 & 0 \\ 0 & x & y \\ -C & A - C & B - C \end{vmatrix}.$$

Computing the determinant with

$$(0, 0) = l - 8 + c, \qquad (0, 1) = (1, 0), \qquad (0, 2) = (1, 1)$$

we obtain the indicial form. We summarize the results in the following

Proposition 3 *Let $\beta \in O_K$. Then the index of β is given by*

$$\pm\mathrm{Ind}(\beta) = dx^3 + \left(\frac{-c - 3d}{2}\right)x^2y + \left(\frac{c - 3d}{2}\right)xy^2 + dy^3$$

where $4l = c^2 + 27d^2$, $c \equiv 1 \pmod 3$, $d > 0$, and $\beta = x\alpha + y\sigma(\alpha)$.

This representation for the indicial form gives immediately an upper bound for $m(K)$. For $x = 1$, $y = 0$, we have $\mathrm{Ind}(\alpha) = d$. Hence $m(K) \leq (4l/27)^{1/2}$.

The question of the existence of a power basis is reduced to considering whether this form represents 1 (note that if the form represents ± 1 then it represents 1). Direct numerical tabulation of values represented by this form allows us to determine power bases in some cases, for example $l = 241$ $(x = -1,\ y = 2)$, 373 $(x = -2,\ y = 3)$, 379 $(x = -1,\ y = 3)$, 463 $(x = -1,\ y = 2)$, 751 $(x = -1,\ y = 3)$.

Proposition 4 *2 splits (completely) in the extension K if and only if 2 divides d.*

Proof Since α, $\sigma(\alpha)$, $\sigma^2(\alpha)$ are a Z-basis for O_K, their images under the map $O_K \to O_K/\mathfrak{p}$ generate $O_K/\mathfrak{p}$ over Z/pZ. Suppose 2 divides d. Then discriminant$(f_\alpha(x)) \equiv 0 \pmod 2$, so $f_\alpha(x)$ has a multiple root mod 2, hence splits completely mod 2 (a cubic having a multiple root has all its roots in the ground field). Thus $\bar{\alpha}$, $\overline{\sigma(\alpha)}$, $\overline{\sigma^2(\alpha)} \in Z/2Z$, i.e., $[O_K/\mathfrak{p}_2 : Z/2Z] = 1$. Hence $f(\mathfrak{p}_2/(2)) = 1$, and 2 splits in K. Suppose now that d is not divisible by 2 and 2 splits in K. Then $f_\alpha(x)$ must split completely into distinct linear factors mod 2, clearly impossible.

Theorem 1 (Dedekind) *If* $d \equiv 0 \pmod 2$, *then no power basis exists, and in fact every index is divisible by* 2.

Proof This follows immediately from the Dedekind test and the above proposition. We may also see this directly from the indicial form as follows: $4l = c^2 + 27d^2$ implies c and d have the same residue class mod 2. Hence if d is even, c is also. Writing the indicial form as

$$d(x^3 + y^3) - c\left(\frac{x^2y - xy^2}{2}\right) - 3d\left(\frac{x^2y + xy^2}{2}\right)$$

and noting $x^2y + xy^2 \equiv x^2y - xy^2 \equiv 0 \pmod 2$ for all values of x and y, we see that the form is always even.

Remark By Hensel's result above, 2 is a common index divisor in cubic fields if and only if 2 splits completely in the extension. By a result of Engstrom [6], 2^1 is the only possible common index divisor in cubic fields, e.g., 4 never occurs as a common index divisor. References [2, 4, 6, 9, 15] yield a fairly complete history of the results on common index divisors.

Lemma 1 *Let* p *be a prime* $\equiv 1 \pmod 3$ *and let* ρ *be a primitive third root of unity* mod p. *Let* a *be any nonzero residue* mod p. *Suppose* $a^{-1}d$ *is a cubic nonresidue* mod p *and that* $c \equiv (6\rho^2 + 3)d$ mod p. *Then the indicial form does not represent* a.

Proof For $c \equiv (6\rho^2 + 3)d \bmod p$, the indicial form becomes

$$f(x, y) \equiv dx^3 + 3\rho dx^2y + 3\rho^2 dxy^2 + dy^3$$

since $1 + \rho \equiv -\rho^2 \bmod p$. Hence,

$$f(x, y) \equiv d(x + \rho y)^3 \bmod p$$

and the values assumed by the indicial form lie in the same cubic residue class as d. Since a and d lie in distinct cubic classes by assumption, a is not represented by the form.

Using Lemma 1 we are able to construct an infinite class of fields that do not satisfy the conditions necessary for the Dedekind test but which nevertheless do not have a power basis. This set of fields is constructed in such a way that the minimal index $m(K)$ is unbounded as K ranges over the set. That the minimal index is unbounded over the set of pure cubic fields is a result of Hall [9]; the following shows that the same is true for the set of cyclic cubic fields. We shall need the following special case of the generalized Dirichlet theorem. For the proof as a consequence of the Tchebotarev density theorem, see Bass *et al.* [1].

Theorem *Let F be a number field. Given nonzero $a, b \in O_F$ and a nonzero ideal $\mathfrak{A}$ such that $aO_F + bO_F = O_F = \mathfrak{A} + bO_F$, there exist infinitely many primes $\mathfrak{p}$ such that $\mathfrak{p}\mathfrak{A} = mO_F$ for some $m \equiv a \pmod{bO_F}$.*

Theorem 2 *Given any $N > 0$, there exists a cubic subfield K of a prime cyclotomic field $K_l = Q(\zeta)$, ζ a primitive lth root of unity, such that $m(K) > N$ and 2 remains prime in O_K.*

The condition that 2 remain prime in O_K, by Proposition 4, implies that the Dedekind test for the nonexistence of a power basis does not apply, i.e., there is no common index divisor.

Proof Let $p_1, \ldots, p_N$ be distinct primes $\equiv 1 \pmod 3$. Let ρ_i be a primitive cube root of 1 mod p_i. Choose d_i so that $i^{-1} \cdot d_i$ is a cubic nonresidue mod p_i, and let $c_i = (6\rho_i^2 + 3)d_i$. By the Chinese remainder theorem, let c and d be solutions to the following system of congruences:

$$c \equiv d \equiv 1 \pmod 2 \qquad c \equiv c_i \pmod{p_i}$$

$$c \equiv 1 \pmod 3 \qquad 3d \equiv d_i \pmod{p_i}.$$

Let now $F = Q(\sqrt{-3})$ in the Dirichlet theorem above, and set

$$a = \frac{c + 3d\sqrt{-3}}{2}, \qquad b = 6\prod_{i=1}^{N} p_i, \qquad \mathfrak{A} = O_F.$$

Since

$$\mathrm{Norm}_{F/Q}(a) = \frac{c^2 + 27d^2}{4} \equiv d_i^2\left(\frac{(6\rho_i^2 + 3)^2 + 3}{4}\right) \bmod p_i \equiv -6d_i^2 \bmod p_i$$

and $d_i \not\equiv 0 \pmod{p_i}$, it follows that (a) is relatively prime to $(\prod_{i=1}^{N} p_i)$. Also

$$\mathrm{Norm}_{F/Q}(a) \equiv 1 \pmod 6$$

so (a) is also prime to (6). Thus

$$(a) + (b) = \mathfrak{A} + (b) = O_F,$$

and by the Dirichlet theorem, there exists a prime $\mathfrak{p}$ such that $\mathfrak{p} = (m)$, where

$$m \equiv \frac{c + 3d\sqrt{-3}}{2} \bmod\left(6\prod_{i=1}^{N} p_i\right).$$

If the prime $\mathfrak{p}$ were of degree 2, then $\mathfrak{p} = (p) = (m)$, where p is a rational prime. Hence $p \sim m$ in O_F. The units of F are ± 1, $\pm\omega$, and $\pm\omega^2$, where $\omega = \frac{1}{2}(1 + \sqrt{-3})$. Hence we would have

$$m = \left(\frac{c + 3d\sqrt{-3}}{2}\right) + 6\prod_{i=1}^{N} p_i\left(\frac{x + y\sqrt{-3}}{2}\right)$$

with $x, y \in Z$, and such that

$$m = \pm p, \ \pm p\omega, \ \pm p\omega^2.$$

The first is impossible since

$$3d + 6y\prod_{i=1}^{N} p_i \equiv 1 \pmod 2,$$

so m cannot be real. The latter two cases would imply

$$m = \frac{\pm p \pm p\sqrt{-3}}{2}$$

which is also impossible since

$$\pm\left(c + 6x\prod_{i=1}^{N} p_i\right) = \pm\left(3d + 6y\prod_{i=1}^{N} p_i\right)$$

is impossible mod 3.

Thus the prime $\mathfrak{p}$ is of first degree, so

$$l = \mathrm{Norm}_{F/Q}(\mathfrak{p})$$

$$= \mathrm{Norm}_{F/Q}\left(\frac{(c + 6\prod_{i=1}^{N} p_i \cdot x) + (3d + 6\prod_{i=1}^{N} p_i \cdot y)}{2}\sqrt{-3}\right) = \frac{s^2 + 27t^2}{4}$$

is a rational prime with

$$s \equiv t \equiv 1 \pmod 2$$

$$s \equiv c_i \pmod{p_i}, \qquad t \equiv d_i \pmod{p_i}.$$

Let K be the cubic subfield of the prime cyclotomic field K_l for this l. The numbers $1, \ldots, N$ do not occur as indices by Lemma 1, and 2 remains prime in K by Proposition 4.

The indicial form and the integers it represents can also be connected with a certain norm form in the cubic field K. Letting $\beta = x\alpha + y\sigma(\alpha)$, we know

$$D(1, \beta, \beta^2) = \mathrm{Ind}(\beta)^2 \cdot D(K),$$

or since $D(K) = l^2$,

$$\mathrm{Ind}(\beta)^2 \cdot l^2 = N(\delta(\beta)).$$

The prime l is totally ramified in K, and the prime sitting above l in K is principal, say

$$l = \mathfrak{p}^3 = (\gamma)^3$$

(γ can be taken to be the relative norm from K_l to K of $1 - \zeta$). Since l is

totally ramified, we can also write

$$l^2 = \mathrm{Norm}_{K/Q}(\gamma)^2 = \mathrm{Norm}(\gamma\sigma^2(\gamma)).$$

Letting $\delta(\beta) = (\beta - \sigma(\beta))(\beta - \sigma^2(\beta))$, we have

$$\mathrm{Ind}(\beta)^2 = \left| \frac{\mathrm{Norm}(\beta - \sigma(\beta))(\beta - \sigma^2(\beta))}{\mathrm{Norm}(\gamma\sigma^2(\gamma))} \right|$$

$$= \left|\mathrm{Norm}\left(\frac{\beta - \sigma(\beta)}{\gamma}\right)\right| \cdot \left|\mathrm{Norm}\left(\frac{\beta - \sigma^2(\beta)}{\sigma^2(\gamma)}\right)\right|.$$

Applying σ to the second norm, we find that

$$\left|\mathrm{Norm}\left(\frac{\beta - \sigma(\beta)}{\gamma}\right)\right| = \left|\mathrm{Norm}\left(\frac{\beta - \sigma^2(\beta)}{\sigma^2(\gamma)}\right)\right|$$

so that

$$\mathrm{Ind}(\beta) = \left|\mathrm{Norm}_{K/Q}\left(\frac{\beta - \sigma(\beta)}{\gamma}\right)\right|.$$

Note that as l is totally ramified, the inertial group of $\mathfrak{p} = (\gamma)$ is the full galois group, so $\beta \equiv \sigma(\beta) \bmod \mathfrak{p}$ for all σ. Hence the element $(\beta - \sigma(\beta))/\gamma$ is an integer. We write this as

Proposition 5 $\mathrm{Ind}(\beta) = |\mathrm{Norm}_{K/Q}(\xi)|$ *where* $\xi = (\beta - \sigma(\beta))/\gamma \in O_K$.

By this proposition, the existence of certain indices implies certain relations in the class group of K. In particular, in the case of prime indices, we have the following result.

Proposition 6 *Suppose the prime $p \neq l$ is an index in K. Then p splits in K into three principal factors.*

Proof By Proposition 5, $p = \mathrm{Norm}(\xi)$ for some $\xi \in O_K$. Since p is unramified in K, $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, with $f(\mathfrak{p}_i/(p)) = 1$. Further, $(\xi) = \mathfrak{p}_i$ for some i, is principal, and since the $\mathfrak{p}_i$ are conjugate under the Galois group, each $\mathfrak{p}_i$ is principal.

If the structure of the class group is known, Proposition 6 is useful in eliminating certain possible values for $m(K)$. For example, if $l = 277$, then $m(K) = 2$ or 4. Determining the splitting of all primes $p < \frac{1}{7}l$ to determine the class group structure (the constant $\frac{1}{7}$ is due to Davenport [3]), using $f_\alpha(x) = x^3 + x^2 - 92x + 236$ (see the comment following Proposition 2), shows that only 2, 13, 19, and 37 split in K. Since $\mathrm{Norm}(\alpha - 4) = 2^2 \cdot 13$, $\mathrm{Norm}(\alpha - 8) = 2^2 \cdot 19$, and $\mathrm{Norm}(\alpha - 5) = 2 \cdot 37$, we have

$$C_K = \langle [\mathfrak{p}_2], [\mathfrak{p}_2'] \rangle$$

where C_K is the class group of K and $[\mathfrak{p}_2]$, $[\mathfrak{p}_2']$ are the classes of two

(conjugate) primes lying above 2 in K. Since the class number of K can be computed by analytic techniques, and $h(K) = 4$ for this field [8], $\mathfrak{p}_2$ cannot be principal. Hence by Proposition 6, 2 is not an index, so $m(K) = 4$. Similar calculations hold for the prime $l = 397$, but for all other undecided $m(K)$, $l < 1000$, $h(K) = 1$, so Propositions 5 and 6 are of no help.

We remark that the converse of Proposition 6 does not always hold, for example in the case $l = 499$, where $h(K) = 1$, and 2 splits into necessarily principal factors, and yet 2 is not an index (congruence considerations of the indicial form mod 9).

Let now n be a square-free integer, not necessarily prime. If $n \equiv 1 \pmod 3$, then the cyclotomic field K_n has a cubic subfield K of discriminant n^2. By Hasse [10], the element $\alpha = (-1)^{r+1} \operatorname{Tr}_{K_n/K}(\zeta)$ generates a normal basis for O_K, where r is the number of distinct primes dividing n and ζ is a primitive nth root of unity. Further, α has minimal polynomial

$$f_\alpha(x) = x^3 + x^2 - \left(\frac{n-1}{3}\right)x - \left(\frac{nc + 3n - 1}{27}\right)$$

where $4n = c^2 + 27d^2$, $c \equiv 1 \pmod 3$ as in the case for n prime.

Theorem 3 *There exist infinitely many cubic subfields K of cyclotomic fields K_n for which $m(K) = 1$, i.e., a power basis exists for the ring of integers in K.*

Proof The index of α defined above is given by $(D(f_\alpha(x))/D(K))^{1/2}$, and a straightforward computation of $D(f_\alpha(x))$ shows α has index d. Hence it suffices to show there exist infinitely many square-free integers n such that $4n = c^2 + 27$, or equivalently, $n = k^2 + k + 7$ (see Narkiewicz [13]). Let N_x denote the number of square-free integers of the form $k^2 + k + 7$ for $k \le x$. Then $N_x \ge x - M_x$, where M_x denotes the number of integers of the form $k^2 + k + 7$ for $k \le x$ and having a square factor. Hence,

$$M_x = \operatorname{card}\{k \le x \mid k^2 + k + 7 \equiv 0 \pmod{p^2} \text{ for some prime } p\}.$$

We may clearly take $p \le x$. Since the congruence $k^2 + k + 7 \equiv 0 \pmod{p^2}$ has at most two solutions on any residue system except for $p = 3$, we have

$$M_x \le \left(3 \cdot \frac{x}{9} + 3\right) + \sum_{5 \le p \le x} \left(2 \cdot \frac{x}{p^2} + \theta_p\right)$$

where $\theta_p \le 2$. Hence

$$N_x \ge x\left(\frac{2}{3} - 2\sum_{p \ge 5} \frac{1}{p^2}\right) - 2\sum_{p \le x} 1 = Cx + o(x)$$

Since $C = \frac{2}{3} - 2\sum_{p \ge 5} p^{-2} \ge 0$, we have $N_x \to \infty$ as $x \to \infty$, concluding the proof.

The determination of $m(K)$ for any particular case reduces to solving a finite number of cubic Diophantine equations, namely $f(x, y) = a$, where $f(x, y)$ is the indicial form and a is a positive integer less than $(4l/27)^{1/2}$. In conclusion, we determine $m(K)$ for the cubic subfield K of K_{181}. We let $N(A)$ denote $\mathrm{Norm}_{K/Q}(A)$.

For $l = 181$, we have $c = 7$, $d = 5$, and the indicial form for this field is

$$f(z, y) = 5z^3 - 11z^2y - 4zy^2 + 5y^3.$$

The prime 3 remains prime in this extension, so by Proposition 6, cannot be an index. Further, for d odd, $m(K)$ is also odd. (*Proof:* The indicial form mod 2 for d odd is either $x^3 + x^2y + y^3$ or $x^3 + xy^2 + y^3$ since one of $-c - 3d$ and $c - 3d$ is $\equiv 0 \pmod 4$ and the other is $\equiv 2 \pmod 4$. Hence, an even index is represented only for $x \equiv y \equiv 0 \pmod 2$. But then $(x\alpha + y\sigma(\alpha))/2$ is an integer with smaller index, a contradiction. Hence $m(K)$ is odd.) Thus $m(K) = 1$ or 5. We shall show $m(K) = 5$ by showing $f(z, y) = 1$ for integers z and y is impossible.

Assume $f(z, y) = 1$, for $z, y \in Z$. Then letting $x = 5z$, we have

$$25 = 25 \cdot f(z, y) = x^3 - 11x^2y - 20xy^2 + 125y^5.$$

By Proposition 5, $f(x, y)$ is always reducible in $K[x, y]$, and in this case we have

$$(25) = (x - \theta y)(x - \sigma(\theta)y)(x - \sigma^2(\theta)y) \tag{1}$$

where $\theta = \alpha + 4$. Define $\mathfrak{p}_5$ by

$$(\alpha - \sigma(\alpha)) = \mathfrak{p}_5 \mathfrak{p}_{181}$$

(recall $\mathrm{Ind}(\alpha) = d = 5$). Since $N(\theta) = -125$, (θ) is divisible by three primes above 5. Also $N(\theta + 5) = -5^2 \cdot 7$. If (θ) were divisible by the three distinct primes above 5 in K, then $(5) \mid (\theta + 5)$ ($\mid$ denotes divisibility), which would imply $5^3 \mid N(\theta + 5)$, a contradiction. If (θ) were the cube of a prime above 5, then $N(\theta + 5)$ would not be divisible by 5^2. Hence $(\theta) = \mathfrak{q}_5^2 \mathfrak{q}_5'$, where $\mathfrak{q}_5$, $\mathfrak{q}_5'$ are two distinct primes lying above 5 in K. Since $(\theta - \sigma(\theta)) = (\alpha - \sigma(\alpha))$, we have by definition of $\mathfrak{p}_5$, $\mathfrak{p}_5 \mid (\theta - \sigma(\theta))$, and considering the possibilities for $\mathfrak{q}_5$ and $\mathfrak{q}_5'$, we see that only $(\theta) = \mathfrak{p}_5^2 \mathfrak{p}_5''$ and $(\theta) = (\mathfrak{p}_5'')^2 \mathfrak{p}_5$ are possible, where $\mathfrak{p}_5' = \sigma(\mathfrak{p}_5)$ and $\mathfrak{p}_5'' = \sigma^2(\mathfrak{p}_5)$. In either case, since $5 \mid x$, we have

$$\mathfrak{p}_5 \mathfrak{p}_5'' \mid (x - y\theta)$$

and since $N(x - y\theta) = 25$,

$$(x - y\theta) = \mathfrak{p}_5 \mathfrak{p}_5''. \tag{2}$$

An integral basis for this field is given by α, $\sigma(\alpha)$, and $\sigma^2(\alpha)$, or in terms of

the computationally easier 1, α, α^2,

$$\sigma(\alpha) = \left(\frac{38 - 2\alpha - \alpha^2}{5}\right), \qquad \sigma^2(\alpha) = \left(\frac{-43 - 3\alpha + \alpha^2}{5}\right).$$

There are two conjugate fundamental units for this field, given by

$$\varepsilon_1 = \left(\frac{26 + 21\alpha - 2\alpha^2}{5}\right), \qquad \varepsilon_2 = \left(\frac{54 - 16\alpha - 3\alpha^2}{5}\right)$$

(these units were originally calculated by the method of Godwin [7], and are the same units given in the tables of Gras [8]).

We may calculate $\mathfrak{p}_5$ explicitly from $(\alpha - \sigma(\alpha)) = \mathfrak{p}_5\,\mathfrak{p}_{181}$ to be

$$\mathfrak{p}_5 = \left(\frac{2 - 8\alpha + \alpha^2}{5}\right)$$

with conjugates

$$\mathfrak{p}_5' = \left(\frac{7 + 7\alpha + \alpha^2}{5}\right), \qquad \mathfrak{p}_5'' = \left(\frac{126 + \alpha - 2\alpha^2}{5}\right).$$

Hence, from Eq. (2), we have

$$\begin{aligned} x - y\theta &= \varepsilon_1^n \varepsilon_2^m (\tfrac{1}{5})^2 (2 - 8\alpha + \alpha^2)(126 + \alpha - 2\alpha^2) \\ x - y\sigma(\theta) &= \varepsilon_1^{-m} \varepsilon_2^{n-m} (\tfrac{1}{5})^2 (7 + 7\alpha + \alpha^2)(2 - 8\alpha + \alpha^2) \\ x - y\sigma^2(\theta) &= \varepsilon_1^{m-n} \varepsilon_2^{-n} (\tfrac{1}{5})^2 (126 + \alpha - 2\alpha^2)(7 + 7\alpha + \alpha^2) \end{aligned} \tag{3}$$

where we have used the fact that ε_1 and ε_2 are conjugates to obtain the second two equations, and where m and n are integers.

We shall show the equations in (3) are impossible by considering them first modulo $\mathfrak{p}_7$ (a prime lying above 7 in K) and then modulo $\mathfrak{p}_{19}$ (similarly a prime lying above 19 in K). Note that $N(\alpha - 2) = 5^2 \cdot 7$ and $N(\alpha - 7) = 5 \cdot 19$, so that both $\mathfrak{p}_7$ and $\mathfrak{p}_{19}$ are first degree primes in K, which may be defined as the kernels of the homomorphisms $O_K \to Z/7Z$ (by $\alpha \to 2$) and $O_K \to Z/19Z$ (by $\alpha \to 7$), respectively.

Modulo $\mathfrak{p}_7$, we have, since $\alpha \equiv 2 \pmod{\mathfrak{p}_7}$,

$$\varepsilon_1 \equiv 5 \pmod{\mathfrak{p}_7}, \qquad \varepsilon_2 \equiv 2 \pmod{\mathfrak{p}_7}$$

$$\left(\frac{2 - 8\alpha + \alpha^2}{5}\right) \equiv 5 \pmod{\mathfrak{p}_7}$$

$$\left(\frac{7 + 7\alpha + \alpha^2}{5}\right) \equiv 5 \pmod{\mathfrak{p}_7}$$

$$\left(\frac{126 + \alpha - 2\alpha^2}{5}\right) \equiv 3 \pmod{\mathfrak{p}_7}$$

$$\theta = \alpha + 4 \equiv 6 \pmod{\mathfrak{p}_7}, \qquad \sigma(\theta) \equiv 3 \pmod{\mathfrak{p}_7},$$

and

$$\sigma^2(\theta) \equiv 2 \pmod{\mathfrak{p}_7}.$$

Hence Eq. (3) becomes

$$\begin{aligned} x + y &\equiv 5^n 2^m \equiv (-1)^n 2^{n+m} \pmod{\mathfrak{p}_7} \\ x - 3y &\equiv 5^{-m} 2^{n-m} 4 \equiv (-1)^m 2^{n-2m} 4 \pmod{\mathfrak{p}_7} \\ x - 2y &\equiv 5^{m-n} 2^{-n} \equiv (-1)^{n+m} 2^{m-2n} \pmod{\mathfrak{p}_7}. \end{aligned} \tag{4}$$

Then

$$\frac{x-2y}{x+y} \equiv (-1)^m \pmod{\mathfrak{p}_7}, \qquad \frac{x-2y}{x-3y} \equiv (-1)^n \cdot 2 \pmod{\mathfrak{p}_7}$$

imply that m is odd and n is even (m even implies $y \equiv 0 \pmod 7$, and the indicial form does not represent 1 for such y, and m odd implies $x \equiv 4y \pmod{\mathfrak{p}_7}$, which shows $(x-2y)/(x-3y) \equiv 2 \pmod{\mathfrak{p}_7}$, i.e., n is even).

We now consider Eqs. (3) mod $\mathfrak{p}_{19}$, where $\alpha \equiv 7 \pmod{\mathfrak{p}_{19}}$. We have here

$$\varepsilon_1 \equiv 15 \pmod{\mathfrak{p}_{19}}, \qquad \varepsilon_2 \equiv 16 \pmod{\mathfrak{p}_{19}}$$

$$\left(\frac{2 - 8\alpha + \alpha^2}{5}\right) \equiv 18 \pmod{\mathfrak{p}_{19}}$$

$$\left(\frac{7 + 7\alpha + \alpha^2}{5}\right) \equiv 2 \pmod{\mathfrak{p}_{19}}$$

$$\left(\frac{126 + \alpha - 2\alpha^2}{5}\right) \equiv 7 \pmod{\mathfrak{p}_{19}}$$

$$\theta \equiv 11 \pmod{\mathfrak{p}_{19}}, \qquad \sigma(\theta) \equiv -1 \pmod{\mathfrak{p}_{19}}, \qquad \sigma^2(\theta) \equiv 1 \pmod{\mathfrak{p}_{19}}.$$

Here we have

$$\begin{aligned} x - 11y &\equiv 15^n 16^m 12 \pmod{\mathfrak{p}_{19}} \\ x + y &\equiv 15^{-m} 16^{n-m} 17 \pmod{\mathfrak{p}_{19}} \\ x - y &\equiv 15^{m-n} 16^{-n} 14 \pmod{\mathfrak{p}_{19}}. \end{aligned}$$

Since n is even, m odd, set $n = 2k_1$ and $m = 2k_2 + 1$. Then the first two equations become

$$\begin{aligned} x - 11y &\equiv (15^2)^{k_1} (16)^{2k_2} \cdot 2 \pmod{\mathfrak{p}_{19}} \\ x + y &\equiv (15^2)^{-k_2} (16)^{2k_1 - 2k_2} \cdot 3 \pmod{\mathfrak{p}_{19}}. \end{aligned}$$

Now, 2 is a quadratic nonresidue mod $\mathfrak{p}_{19}$, as is 3 (the quadratic residues

TABLE 1

l	c	d	A	B	$m(K)$	l	c	d	A	B	$m(K)$
7	1	1	−2	−1	1	439	28	6	−23	5	6
13	5	1	−4	1	1	457	10	8	−17	−7	2, 4, 8
19	7	1	−5	2	1	463	23	7	−22	1	1
31	4	2	−5	−1	2	487	25	7	−23	2	5, 7
37	11	1	−7	4	1	499	32	6	−25	7	4, 6
43	8	2	−7	1	2	523	43	3	−26	17	3
61	1	3	−5	−4	1	541	29	7	−25	4	1, 7
67	5	3	−7	−2	3	547	1	9	−14	−13	1
73	7	3	−8	−1	3	571	31	7	−26	5	7
79	17	1	−10	7	1	577	11	9	−19	−8	3, 9
97	19	1	−11	8	1	601	26	8	−25	1	2
103	13	3	−11	2	3	607	49	1	−26	23	1
109	2	4	−7	−5	2	613	47	3	−28	19	3
127	20	2	−13	7	2	619	17	9	−22	−5	1, 3
139	23	1	−13	10	1	631	43	5	−29	14	1, 5
151	19	3	−14	5	1, 3	643	40	6	−29	11	4, 6
157	14	4	−13	1	2	661	49	3	−29	20	3
163	25	1	−14	11	1	673	37	7	−29	8	1, 7
181	7	5	−11	−4	5	691	8	10	−19	−11	2, 4, 8
193	23	3	−16	7	3	709	53	1	−28	25	1
199	11	5	−13	−2	1, 5	727	44	6	−31	13	6
211	13	5	−14	−1	1, 5	733	50	4	−31	19	2, 4
223	28	2	−17	11	2	739	16	10	−23	−7	2, 4, 8, 10
229	22	4	−17	5	2, 4	751	41	7	−31	10	1
241	17	5	−16	1	1	757	29	9	−28	1	3
271	29	3	−19	10	3	769	49	5	−32	17	1, 5
277	26	4	−19	7	4	787	31	9	−29	2	3
283	32	2	−19	13	2	811	56	2	−31	25	2
307	16	6	−17	−1	2, 6	823	5	11	−19	−14	1, 5
313	35	1	−19	16	1	829	7	11	−20	−13	7
331	1	7	−11	−10	1	853	35	9	−31	4	1, 9
337	5	7	−13	−8	1, 5	877	59	1	−31	28	1
349	37	1	−20	17	1	883	47	7	−34	13	1, 7
367	35	3	−22	13	3	907	19	11	−26	−7	1, 11
373	13	7	−17	−4	1	919	52	6	−35	17	2, 6
379	29	5	−22	7	1	937	61	1	−32	29	1
397	34	4	−23	11	4	967	41	9	−34	7	3, 9
409	31	5	−23	8	1, 5	991	61	3	−35	26	3
421	19	7	−20	−1	1, 7	997	10	12	−23	−13	6, 8, 10
433	2	8	−13	−11	2						

are 1, 4, 5, 6, 7, 9, 11, 16, 17), so both $x - 11y$ and $x + y$ are quadratic nonresidues. Tabulating the pairs (z, y) for which $f(z, y) \equiv 1 \pmod{19}$, we find that for no pairs are $5z - 11y$ and $5z + y$ both nonresidues. Hence the equations (3) are impossible, and $m(K) = 5$.

Table 1 lists the indicial form coefficients (as $dx^3 + Ax^2y + Bxy^2 + dy^3$), and the known $m(K)$ for $l < 1000$. In the cases where several indices are listed, they are the only possible values for $m(K)$ but it is undetermined which is correct. Except for the case $l = 181$ above, these values were obtained by Proposition 6 (using the tables of Gras [8] for the class numbers) and by congruence considerations of the indicial form. Note that c has been normalized positive in the table and that this does not affect the values assumed by the indicial form.

Finally, we wish to acknowledge the assistance of George Cooke for helpful suggestions and comments.

REFERENCES

[1] H. Bass, J. Milnor, and J.-P. Serre, Solution of the congruence subgroup problem for Sl_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$), *Inst. Hautes Études Sci. Publ. Math.* **33** (1967), 83–84.

[2] N. Bauer, Über den ausserwesentlicher Discriminantenteiler algebraischer Körper, *Math. Ann.* **64** (1907), 573.

[3] H. Davenport, On the product of three homogeneous linear forms III, *Proc. London Math. Soc.* **45** (1939), 98–125.

[4] R. Dedekind, Über den Zussamenhang zwischen der Theorie der Ideals und der Theorie der höheren Kongruenzen, *Abh. Akad. Wiss. Göttingen, Math.-Phys. Kl.* **23** (1878), 1–23.

[5] L. E. Dickson, Cyclotomy, higher congruences and Waring's problem, *Amer. J. Math.* **57** (1935), 393.

[6] H. T. Engstrom, On the common index divisors of an algebraic field, *Trans. Amer. Math. Soc.* **32** (1930), 223–237.

[7] H. J. Godwin, The determination of units in totally real cubic fields, *Proc. Cambridge Philos. Soc.* **56** (1960), 318–321.

[8] Marie N. Gras, Methodes et algorithmes pour le calcul numerique du nombre de classes et des unites des extensions cubiques cycliques de Q, Universite Scientifique et Medicale de Grenoble, 1972.

[9] Marshall Hall, Jr., Indices in cubic fields, *Bull. Amer. Math. Soc.* **43** (1937), 104–108.

[10] H. Hasse, Arithmetische Bestimmungen von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern, *Abh. Deutsch. Akad. Wiss. Berlin Kl. Math. Phys. Tech.* 1948 (1950), nr. 2.

[11] K. Hensel, Arithmetische Untersuchungen über die gemeinsamer ausserwesentlicher Discriminantenteiler einer Gattung, *J. für Math.* **113** (1894), 128–160.

[12] Serge Lang, "Algebraic Number Theory." Addison Wesley, Menlo Park, California, 1970.

[13] M. Narkiewicz, "Elementary and Analytic Theory of Algebraic Numbers," p. 389. Polish Scientific Publishers, Warsaw, 1974.

[14] Thomas Storer, "Cyclotomy and Difference Sets." Markham, Chicago, 1967.

[15] E. von Zylinsky, Zur Theorie der ausserwesentlicher Discriminantenteiler algebraischer Körper, *Math. Ann.* **73** (1913), 273–274.

AMS (MOS) 1970 subject classification: 12A30.

Spinor Genera under Field Extensions, III: Quadratic Extensions

A. G. EARNEST† *J. S. HSIA*

THE OHIO STATE UNIVERSITY
COLUMBUS, OHIO

It has been shown by the authors that any two integral quadratic forms in the same genus over the rational number field which are not properly spinor equivalent do not become properly spinor equivalent in any odd-degree extension of $\mathbb{Q}$ (see Earnest and Hsia [7]). But examples given in Earnest and Hsia [4, 6] have indicated that this type of behavior cannot, in general, be expected for quadratic extensions. It is the purpose of this paper to give *constructive* methods for determining the amount of collapsing of proper spinor genera in quadratic extensions of $\mathbb{Q}$. Additionally, several results are obtained giving information about the *number* of proper spinor genera in the genus of the lifted lattice.

The vehicle used in studying the lifting behavior of spinor genera is the correspondence, first described by Kneser in [11], between the proper spinor genera and a factor group of the idèle group of the coefficient field. The noncollapsing of the proper spinor genera in odd-degree extensions can be established by showing the injectivity of the natural lifting map between the corresponding idèle groups. In the case of quadratic extensions, however, the

† Present address: University of Southern California, Los Angeles, California.

kernel of this map may be nontrivial and it is this kernel that we shall compute in Section 1. Of course, in order to determine the idèle groups involved, it is first necessary to compute the local spinor norm groups of the lattice under consideration. This can be carried out for the spots on the rational number field using techniques from Kneser [11] and Earnest and Hsia [5]. However, these spinor norms have not previously been determined for the dyadic spots on quadratic fields. While the general problem of calculating the spinor norm groups over arbitrary dyadic local fields is extremely difficult, it is possible to use the strong local condition that the ramification degree is less than or equal to 2 to extend the results of Hsia [9] and Earnest and Hsia [5] to perform the necessary calculations for quadratic fields. This is done in Section 2.

The third section of this paper shows several applications of the techniques of the first two sections. Examples of $\mathbb{Z}$-lattices and quadratic extensions are constructed showing that the number of spinor genera which collapse may be any arbitrary 2-power. We give a condition sufficient to assure that, while distinct proper spinor genera from the genus of a $\mathbb{Z}$-lattice L may collapse in the genus of the lattice $\tilde{L}$ lifted to a quadratic extension, the *number* $g^+(\tilde{L})$ of proper spinor genera in $\text{gen}(\tilde{L})$ is no smaller than the number $g^+(L)$ in $\text{gen}(L)$. The condition is satisfied, in particular, when there is no rational prime that divides *both* the discriminant of the field extension and the determinant of the lattice. Finally, the computations appearing in Section 2 are applied to give sufficient conditions, in terms of the reduced determinant of L, for the number $g^+(\tilde{L})$ to be smaller than or equal to the order of the 2-Sylow subgroup of the ideal class group of the quadratic field. Of course, if the class number of the field is odd, this gives $g^+(\tilde{L}) = 1$.

The techniques described in Section 1 are easily adaptable to the use of computer methods for the calculation of the kernel of the lifting maps. A sample of data obtained with the use of the IBM System 370 at the Ohio State University is contained in the first author's doctoral dissertation [2]. Further results will appear in a future paper, written jointly with John H. Yang.

We now recall briefly the notation established in our previous papers dealing with spinor genus behavior. Unexplained notations can be found in O'Meara [12] and Earnest and Hsia [6]. With the exception of Section 2, L will denote a $\mathbb{Z}$-lattice and $\tilde{L} = L \otimes_{\mathbb{Z}} \mathfrak{o}$ the lattice lifted to the quadratic extension $E = \mathbb{Q}(\sqrt{m})$ (here $\mathfrak{o}$ denotes the ring of algebraic integers of E). The proper spinor genera in the genus of L correspond bijectively to the elements of the factor group $J_V/P_V J'_V J_L$, where V denotes the quadratic space on which L is defined. The spinor norm map induces an injective map

$$\phi_L: J_V/P_V J'_V J_L \to J_{\mathbb{Q}}/P_D J^L_{\mathbb{Q}} = \mathscr{G}_{\mathbb{Q}}(L)$$

which is in fact an isomorphism when $\dim L \geq 3$. The corresponding groups can be considered over the extension E and for any prime spot $\mathfrak{p}$ on E lying over p, the lifting maps $g: J_{\mathbb{Q}} \to J_E$ and $h: J_V \to J_{\mathfrak{p}}$, defined respectively by

$$(g(j_p))_{\mathfrak{p}} = j_p \qquad \text{and} \qquad (h(\sigma_p))_{\mathfrak{p}} = \sigma_p \otimes E_{\mathfrak{p}}$$

induce homomorphisms ψ_L and Γ_L in the commutative diagram

$$\begin{array}{ccc} J_{\mathfrak{p}}/P_{\mathfrak{p}}J'_{\mathfrak{p}}J_L & \xrightarrow{\phi_L} & \mathscr{G}_{E(L)} \\ \Gamma_L \uparrow & & \uparrow \psi_L \\ J_V/P_V J'_V J_L & \xrightarrow{\phi_L} & \mathscr{G}_{\mathbb{Q}}(L). \end{array}$$

Upon determining $\mathrm{Ker}(\psi_L)$, it is possible to relate directly back to the collapsing behavior of spinor genera by using the method outlined in Appendix B of [7].

1. Computation of $\mathrm{Ker}(\psi_L)$

The problem of computing $\mathrm{Ker}(\psi_L)$ is twofold. First, we need to identify a set of elements of $J_{\mathbb{Q}}$ whose classes modulo $P_D J_{\mathbb{Q}}^L$ give a complete list of the elements of $\mathscr{G}_{\mathbb{Q}}(\tilde{L})$ (since $\dim L \geq 3$, this set is finite). Second, we need an effective way to determine for a particular $j \in J_{\mathbb{Q}}$ whether $\psi_L(\bar{j}) = (\bar{1}) \in \mathscr{G}_E(\tilde{L})$ or, equivalently, whether $h(j) \in P_{\mathfrak{D}} J_E^L$ (h denotes the map of $J_{\mathbb{Q}}$ into J_E that induces ψ_L). These two questions are closely related and will be treated with similar techniques. To determine whether $\bar{j}$ equals $(\bar{1})$ in $\mathscr{G}_{\mathbb{Q}}(L)$, we need to check whether there is some element α of D for which $\alpha j \in J_{\mathbb{Q}}^L$. Since there are an infinite number of possible choices for such α, the problem is essentially that of finding some finite subset of elements of D that represent all possible cosets of the elements of D modulo $J_{\mathbb{Q}}^L$. The second problem can be likewise reduced to finding a finite subset of elements of $\tilde{D}$ that represent all possible cosets of elements of $\tilde{D}$ modulo J_E^L.

We deal first with the question of determining representatives for the elements of $\mathscr{G}_{\mathbb{Q}}(L)$. There are two subsets of the set S consisting of all finite rational primes; these are related to the lattice L and are important for this investigation. Denote the set of "exceptional" primes for L by

$$\mathscr{E}(L) = \{p \in S: \theta(O^+(L_p)) \neq u_p \dot{\mathbb{Q}}_p^2\}.$$

We distinguish also a subset of $\mathscr{E}(L)$ that consists of those primes that will be used as "multipliers"; let

$$\mathscr{M}(L) = \{p \in S: \theta(O^+(L_p)) \not\subseteq u_p \dot{\mathbb{Q}}_p^2\}.$$

Note that $\mathscr{M}(L) \subseteq \mathscr{E}(L)$ and that both sets consist of only finitely many primes. The significance of these sets lies in the following proposition.

Proposition 1.1 (i) *Let L be definite and $j \in J_{\mathbb{Q}}^S$. Then $\bar{j} = (\bar{1}) \in \mathscr{G}_{\mathbb{Q}}(L)$ if and only if there is some $m = \prod_{p \in \mathscr{M}(L)} p^{\varepsilon_p}$, with $\varepsilon_p \in \{0, 1\}$ for each p, for which*

$$mj_p \in \theta(O^+(L_p)) \qquad \text{for all} \quad p \in \mathscr{E}(L).$$

(ii) *Let L be indefinite and $j \in J_{\mathbb{Q}}^S$. Then $\bar{j} = (\bar{1}) \in \mathscr{G}_{\mathbb{Q}}(L)$ if and only if there is some $m = \pm\prod_{p \in \mathscr{M}(L)} p^{\varepsilon_p}$, with $\varepsilon_p \in \{0, 1\}$ for each p, for which*

$$mj_p \in \theta(O^+(L_p)) \qquad \text{for all} \quad p \in \mathscr{E}(L).$$

Proof of (i) ($\Leftarrow$) For $p \in \mathscr{E}(L)$, we have $mj_p \in \theta(O^+(L_p))$ by assumption. For all p discrete, $p \notin \mathscr{E}(L)$, we have $m \in \mathrm{u}_p$ and $j_p \in \mathrm{u}_p$ by choice of j and by the form of m. Thus, for such p, $mj_p \in \mathrm{u}_p \subseteq \mathrm{u}_p \dot{\mathbb{Q}}_p^2 = \theta(O^+(L_p))$ by the definition of $\mathscr{E}(L)$. So, $mj \in J_{\mathbb{Q}}^L$ and $j \in P_D J_{\mathbb{Q}}^L$.

($\Rightarrow$) Since $\bar{j} = \bar{1}$, there is some $\alpha \in D$ for which $\alpha j \in J_{\mathbb{Q}}^L$. Write $\alpha = \prod_{p \in S} p^{v_p}$, $v_p \in \mathbb{Z}$. For any $p \notin \mathscr{M}(L)$, v_p must be even since $j_p \in \mathrm{u}_p$ and $\theta(O^+(L_p)) \subseteq \mathrm{u}_p \dot{\mathbb{Q}}_p^2$. So α can be rewritten $\alpha = \prod_{p \in \mathscr{M}(L)} p^{\varepsilon_p} \alpha_0^2$ where

$$\alpha_0 \in \dot{\mathbb{Q}} \qquad \text{and} \qquad \varepsilon_p = \begin{cases} 0 & \text{if} \quad v_p \text{ even} \\ 1 & \text{if} \quad v_p \text{ odd.} \end{cases}$$

If $\alpha' = \prod_{p \in \mathscr{M}(L)} p^{\varepsilon_p}$, then $\alpha' j \in J_{\mathbb{Q}}^L$ as desired.

The proof of (ii) is identical except that in the indefinite case $P_D = P_{\mathbb{Q}}$ and so -1 must be included as a possible factor. QED

Consider an arbitrary nontrivial element of $\mathscr{G}_{\mathbb{Q}}(L)$, say $\bar{j}$ for some $j \in J_{\mathbb{Q}}$. The representative j may be changed via multiplication by an element of P_D without changing the class $\bar{j}$. So $\bar{k} = \bar{j}$ where $k \in J_{\mathbb{Q}}^S$ is defined by $k = \prod_{p \in S} p^{-\mathrm{ord}_p(j_p)} j$. Thus, a representative of each element of $\mathscr{G}_{\mathbb{Q}}(L)$ can be chosen from $J_{\mathbb{Q}}^S$. Furthermore, for $j, k \in J_{\mathbb{Q}}^S$, if $j_p \in k_p \dot{\mathbb{Q}}_p^2$ for all $p \in \mathscr{E}(L)$, then $\bar{j} = \bar{k}$. Define the set $\mathscr{E}'(L)$ by $\mathscr{E}'(L) = \{p \in \mathscr{E}(L) \colon \theta(O^+(L_p)) \neq \dot{\mathbb{Q}}\}$. So it suffices to consider only the square classes of the coordinates at the primes p in $\mathscr{E}'(L)$. Thus, a set of representatives of the nontrivial elements of $\mathscr{G}_{\mathbb{Q}}(L)$ is contained in the set of elements $j \in J_{\mathbb{Q}}^S$ satisfying

$$j_p = \begin{cases} 1 & \text{if} \quad p \notin \mathscr{E}'(L) \\ \lambda_p & \text{if} \quad p \in \mathscr{E}'(L) \end{cases} \qquad (*)$$

where, for p odd, λ_p is either 1 or Δ_p (the fixed nonsquare unit of $\mathbb{Q}_p$), and λ_2 is one of the elements 1, 3, 5, or 7. Moreover, to determine whether two such idèles represent distinct classes, it is sufficient to check whether there exists some $m = \pm\prod_{p \in \mathscr{M}(L)} p^{\varepsilon_p}$, with $\varepsilon_p \in \{0, 1\}$ and -1 is used only when L is indefinite, for which $j_p \in mk_p \theta(O^+(L_p))$ for all $p \in \mathscr{E}'(L)$.

The procedure for determining a list of representatives of the classes of $\mathscr{G}_Q(L)$ can now be outlined. After determining the set $\mathscr{E}'(L)$, we consider the list $h_1, \ldots, h_r$ of elements of $J_{\mathbb{Q}}^S$ described by (*). We wish to eliminate redundancies from this list to obtain exactly one representative for each distinct class modulo $P_D J_{\mathbb{Q}}^L$. Let $m_1 = 1, m_2, \ldots, m_s$ be a list of the integers of the form $\pm\prod_{p \in \mathscr{M}(L)} p^{\varepsilon_p}$, where $\varepsilon_p \in \{0, 1\}$ and -1 is used only when L is indefinite, which are pairwise distinct modulo $J_{\mathbb{Q}}^L$. Then $m_2 h_1, \ldots, m_s h_1$ are equivalent to distinct elements of the list $h_2, \ldots, h_r$. These elements can be removed from the list because $\overline{m_i h_1} = \overline{h_1}$. Let u be the smallest index j for which h_j has not been removed from the list; eliminate all the multiples $m_2 h_u, \ldots, m_s h_u$. Eliminating successively in this manner, a list of elements distinct modulo $P_D J_{\mathbb{Q}}^L$ is obtained in a finite number of steps.

Example 1.2 Consider the lattice $L = \langle 1, \alpha^2, 7\alpha^4 \rangle$, where

$$\alpha = 3 \cdot 5 \cdot 19.$$

Local computations show that $\theta(O^+(L_p)) = u_p \dot{\mathbb{Q}}_p^2$ for $p \neq 2, 3, 7$, or 19, $\theta(O^+(L_3)) = \dot{\mathbb{Q}}_3^2$, $\theta(O^+(L_7)) = \dot{\mathbb{Q}}_7$, $\theta(O^+(L_{19})) = \dot{\mathbb{Q}}_{19}^2$, and

$$\theta(O^+(L_2)) = \dot{\mathbb{Q}}_2 .$$

Thus, $\mathscr{M}(L) = \{2, 7\}$, $\mathscr{E}(L) = \{2, 3, 7, 19\}$, and $\mathscr{E}'(L) = \{3, 19\}$. A list of possible representatives of nontrivial classes of $\mathscr{G}_{\mathbb{Q}}(L)$ is formed by j, k, and jk where j and k are defined by

$$j_p = \begin{cases} \Delta_p & \text{if } p = 3 \\ 1 & \text{if } p \neq 3; \end{cases} \qquad k_p = \begin{cases} \Delta_p & \text{if } p = 19 \\ 1 & \text{if } p \neq 19. \end{cases}$$

The list of integers generating principal idèles which are possibly distinct modulo $J_{\mathbb{Q}}^L$ is 1, 2, 7, and 14. Checking coordinatewise, we see that $(2) \equiv jk \pmod{J_{\mathbb{Q}}^L}$ and $(7) \equiv (1) \pmod{J_{\mathbb{Q}}^L}$. So $\overline{jk} = (\bar{1})$ and $j \equiv (2)k \pmod{J_{\mathbb{Q}}^L}$ gives $\bar{j} = \bar{k}$. Hence, $|\mathscr{G}_{\mathbb{Q}}(L)| = 2$ and j is a representative of the nontrivial class.

We now turn to the question of determining for a particular nontrivial element $\bar{j}$ of $\mathscr{G}_{\mathbb{Q}}(L)$ whether or not $\psi_L(\bar{j})$ is a nontrivial element of $\mathscr{G}_E(\tilde{L})$. It is helpful to introduce subsets of the set T of all discrete prime spots of E, which correspond to the set $\mathscr{E}(L)$ and $\mathscr{M}(L)$ in $\mathbb{Q}$. Let

$$\mathscr{E}(\tilde{L}) = \{\mathfrak{p} \in T: \theta(O^+(L_{\mathfrak{p}})) \neq u_{\mathfrak{p}} \dot{E}_{\mathfrak{p}}^2\}$$

and

$$\mathscr{M}(\tilde{L}) = \{\mathfrak{p} \in T: \theta(O^+(L_{\mathfrak{p}})) \not\subseteq u_{\mathfrak{p}} \dot{E}_{\mathfrak{p}}^2\}.$$

Remark 1.3 The set $\mathscr{M}(\tilde{L})$ can be determined from $\mathscr{M}(L)$. Let p be a rational prime and $\mathfrak{p}$ a prime spot on E with $\mathfrak{p} | p$. We make several observations:

(i) If $p \nmid \operatorname{disc}(E/\mathbb{Q})$, then $\theta(O^+(L_p)) \notin \mathfrak{u}_p \dot{\mathbb{Q}}_p^2$ implies $\theta(O^+(\tilde{L}_\mathfrak{p})) \notin \mathfrak{u}_\mathfrak{p} \dot{E}_\mathfrak{p}^2$. Hence, $p \in \mathscr{M}(L)$ implies $\mathfrak{p} \in \mathscr{M}(\tilde{L})$.

(ii) If p is odd and $p \mid \operatorname{disc}(E/\mathbb{Q})$, then $\theta(O^+(\tilde{L}_\mathfrak{p})) \subseteq \mathfrak{u}_\mathfrak{p} E_\mathfrak{p}^2$; hence $\mathfrak{p} \notin \mathscr{M}(\tilde{L})$.

(iii) When $p = 2$, $p \mid \operatorname{disc}(E/\mathbb{Q})$ implies $\theta(O^+(\tilde{L}_\mathfrak{p})) \subseteq \mathfrak{u}_\mathfrak{p} E_\mathfrak{p}^2$ unless $E = \mathbb{Q}(\sqrt{m})$ where $m \equiv 3 \pmod 4$ and L_2 is split by a sublattice of the type $2^r\langle \varepsilon, 2\delta \rangle$, $r \in \mathbb{Z}$, $\varepsilon, \delta \in \mathfrak{u}_2$. This will be verified in Section 2.

We shall now describe the square classes of those elements of $\tilde{D}$ that have even order at all the discrete spots on E. If E is a real quadratic field, let ε denote a fundamental unit of E; if E is imaginary let ε denote the element -1 except when $E = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, in which case $\varepsilon = i$ or $\varepsilon = -\omega_3$, respectively, where ω_3 denotes a cube root of unity.

Proposition 1.4 *Let $\alpha \in E$ with $\operatorname{ord}_\mathfrak{p}(\alpha)$ even for all $\mathfrak{p} \in T$. Let $p_1, \ldots, p_t$ be all the rational primes dividing $\operatorname{disc}(E/\mathbb{Q})$. Then*

$$\alpha \in \pm \varepsilon^{\eta_0} \prod_{i=1}^{t} p_i^{\eta_i} \dot{E}^2$$

for some $\eta_i \in \{0, 1\}$, $i = 0, 1, \ldots, t$.

Proof Consider the ideal $\alpha \mathfrak{o}_E = \mathfrak{A}$. Since $\operatorname{ord}_\mathfrak{p}(\alpha)$ even for all $\mathfrak{p} \in T$, there is some ideal $\mathfrak{B}$ for which $\mathfrak{A} = \mathfrak{B}^2$. If $\mathfrak{B}$ is principal, say $\mathfrak{B} = \beta \mathfrak{o}_E$, then $\alpha = \beta^2 \cdot \gamma$, $\gamma \in \mathfrak{u}_E$. Thus, $\alpha \in \pm \varepsilon^{\eta_0} \dot{E}^2$ for $\eta_0 = 0$ or 1. If $\mathfrak{B}$ is not principal, then $\mathfrak{B}$ is a class of order two in the ideal class group of E. Every ideal class of order two can be represented by an ideal of the form $\prod_{i=1}^t \mathfrak{p}_i^{\eta_i}$, $\eta_i \in \{0, 1\}$ where $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ are the ramified primes of E (for a discussion of this well-known result see, e.g., [10]). It follows that

$$\mathfrak{B} = \left(\prod_{i=1}^{t} \mathfrak{p}_i^{\eta_i} \right) \tau \mathfrak{o}_E \qquad \text{and} \qquad \mathfrak{A} = \mathfrak{B}^2 = \left(\prod_{i=1}^{t} p_i^{\eta_i} \right) \tau^2 \mathfrak{o}_E$$

where $\mathfrak{p}_i \mid p_i$.

So $\alpha = \gamma \tau^2 (\prod_{i=1}^t p_i^{\eta_i})$ with $\gamma \in \mathfrak{u}_E$; that is, $\alpha \in (\pm \varepsilon^{\eta_0})(\prod_{i=1}^t p_i^{\eta_i}) \dot{E}^2$ for $\eta_0 = 0$ or 1. QED

Corollary 1.5 *Let L be a $\mathbb{Z}$-lattice with $\dim L \geq 3$ and let $\alpha \in E$ for which $\operatorname{ord}_\mathfrak{p}(\alpha)$ is even for all $\mathfrak{p} \in T$.*

(i) *If L is indefinite, if $m < 0$, or if $m > 0$ and $N_{E/\mathbb{Q}}(\varepsilon) = +1$, then*

$$\alpha \in \tilde{D} \quad \text{if and only if} \quad \alpha \in \pm \varepsilon^{\eta_0} \left(\prod_{i=1}^{t} p_i^{\eta_i} \right) \dot{E}^2, \quad \eta_i \in \{0, 1\}.$$

(ii) *If L is definite, $m > 0$ and $N_{E/\mathbb{Q}}(\varepsilon) = -1$, then*

$$\alpha \in \tilde{D} \quad \text{if and only if} \quad \alpha \in \pm \left(\prod_{i=1}^{t} p_i^{\eta_i} \right) \dot{E}^2, \quad \eta_i \in \{0, 1\}.$$

Returning now to the computation of $\mathrm{Ker}(\psi_L)$, we take a nontrivial element $\bar{j}$ of $\mathscr{G}_{\mathbb{Q}}(L)$. As in previous arguments, we may choose the representative j from $J_{\mathbb{Q}}^S$. If $\alpha \in \tilde{D}$ is such that $\alpha h(j) \in J_E^L$, we must have $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ even for all $\mathfrak{p} \notin \mathscr{M}(\tilde{L})$, but the order may be arbitrary at those $\mathfrak{p}$ in $\mathscr{M}(\tilde{L})$. So in addition to the elements α described in Corollary 1.5, we must now also consider those α possibly having odd order at some subset of the spots in $\mathscr{M}(\tilde{L})$.

For a set $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_s$ of spots in $\mathscr{M}(\tilde{L})$ we wish to describe those elements α of E satisfying

$$\begin{aligned} &\mathrm{ord}_{\mathfrak{Q}_i}(\alpha) \text{ odd} \qquad \text{for} \quad i = 1, \ldots, s \\ &\mathrm{ord}_{\mathfrak{p}}(\alpha) \text{ even} \qquad \text{for} \quad \mathfrak{p} \neq \mathfrak{Q}_i, \quad i = 1, \ldots, s. \end{aligned} \tag{**}$$

If α and β are two elements both satisfying the conditions (**), then $\mathrm{ord}_{\mathfrak{p}}(\alpha\beta)$ is even for all $\mathfrak{p} \in T$. So the square classes of α and β differ only by a product of those elements obtained in Proposition 1.4. That is, in order to describe the square classes of elements satisfying (**) it suffices to obtain only one such element. The question of the existence of such an element can be settled by an evaluation of Hilbert symbols.

Proposition 1.6 *Let $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_s$ be spots in $\mathscr{M}(\tilde{L})$ with $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_{s'}$ not inert in the extension $E/\mathbb{Q}$. The following statements are equivalent:*

(i) *There exists an element $\alpha \in E$ satisfying (**).*

(ii) $\pm \prod_{i=1}^{s'} q_i \in N_{E/\mathbb{Q}}(\dot{E})$ *where* $q_i \mathbb{Z} = \mathfrak{Q}_i \cap \mathbb{Q}$.

(iii) $\left(\pm \prod_{i=1}^{s'} q_i , m \right)_p = +1$ *for all* $p \in \Omega_{\mathbb{Q}}$.

(iv) $\left(\pm \prod_{i=1}^{s} q_i , m \right)_p = +1$ *for* $p \mid \mathrm{disc}(E/\mathbb{Q})$ *and* $p = 2, q_1, \ldots, q_{s'}$.

Proof (i) $\Rightarrow$ (ii) Let α satisfy (**). Using the formula

$$\mathrm{ord}_p(N_{E/\mathbb{Q}}(\alpha)) = \sum_{\mathfrak{p} \mid p} f(\mathfrak{p} \mid p) \, \mathrm{ord}_{\mathfrak{p}}(\alpha),$$

it follows that $\mathrm{ord}_p(N_{E/\mathbb{Q}}(\alpha))$ is even for those p for which $p \neq q_i$ for any $i = 1, \ldots, s'$. So consider $p = q_i$ for some $i = 1, \ldots, s'$. If p ramifies in E, then $f(\mathfrak{p} \mid p) = 1$ and $\mathrm{ord}_p(N_{E/\mathbb{Q}}(\alpha))$ is odd. If p splits in E, let $\mathfrak{p}, \bar{\mathfrak{p}}$ denote the prime spots lying over p. First, if $\mathfrak{p} = \mathfrak{Q}_i$, $\bar{\mathfrak{p}} = \mathfrak{Q}_j$ for some $i, j = 1, \ldots, s'$ with $i \neq j$, we get $\mathrm{ord}_p(N_{E/\mathbb{Q}}(\alpha)) = \mathrm{ord}_{\mathfrak{Q}_i}(\alpha) + \mathrm{ord}_{\mathfrak{Q}_j}(\alpha)$ is even since both $\mathrm{ord}_{\mathfrak{Q}_i}(\alpha)$ and $\mathrm{ord}_{\mathfrak{Q}_j}(\alpha)$ are odd. On the other hand, if $\bar{\mathfrak{p}} \neq \mathfrak{Q}_j$ for any $j = 1, \ldots, s'$, then $\mathrm{ord}_p(N_{E/\mathbb{Q}}(\alpha))$ is odd since $\mathrm{ord}_{\mathfrak{p}}(\alpha)$ is odd and $\mathrm{ord}_{\bar{\mathfrak{p}}}(\alpha)$ is even. Thus, we can

write $N_{E/\mathbb{Q}}(\alpha) = \pm\prod_{p\in S} p^{\varepsilon_p}$ where ε_p is odd for those p for which $p = q_i$ for some $i = 1, \ldots, s'$ and $p \neq q_j$ for any $i \neq j$, and ε_p is even for all other primes p. The element β has the desired norm where $\beta = \gamma\alpha$ with γ defined by

$$\gamma = \prod_{p\in S} p^{-v_p} \qquad \text{with} \quad v_p = \begin{cases} (\varepsilon_p - 2)/2 & \text{if} \quad p = q_i = q_j, \quad i \neq j \\ (\varepsilon_p - 1)/2 & \text{if} \quad \varepsilon_p \text{ is odd} \\ \varepsilon_p/2 & \text{otherwise.} \end{cases}$$

(ii) $\Rightarrow$ (i) Suppose $\beta \in E$ with $N_{E/\mathbb{Q}}(\beta) = \pm\prod_{i=1}^{s'} q_i$. Distinguish a set U of primes by the following: If $p = q_i$ for some $i = s' + 1, \ldots, s$ and $\mathrm{ord}_{\mathfrak{Q}_i}(\beta)$ is even then $p \in U$; if $p = q_i = q_j$ for $i \neq j$ and $\mathrm{ord}_{\mathfrak{Q}_i}(\beta)$ is even (and thus $\mathrm{ord}_{\mathfrak{Q}_j}(\beta)$ is also even), then $p \in U$; otherwise $p \notin U$. The desired element α satisfying (**) is given by $\alpha = \tau\beta$ where

$$\tau = \prod_{p\in S} p^{v_p}, \qquad v_p = \begin{cases} 0 & \text{if} \quad p \notin U \\ 1 & \text{if} \quad p \in U. \end{cases}$$

(ii) $\Leftrightarrow$ (iii) Let γ denote the element $\pm\prod_{i=1}^{s'} q_i$. Then $\gamma \in N_{E/\mathbb{Q}}(\dot{E})$ if and only if γ is represented over $\mathbb{Q}$ by the quadratic space $[1, -m]$; that is, $[1, -m] \underset{\mathbb{Q}}{\cong} [\gamma, -\gamma m]$. By the classification of rational quadratic forms this isometry condition is equivalent to the equality of the local Hasse symbols $S_p([1, -m]) = S_p([\gamma, -\gamma m])$ for all $p \in \Omega_{\mathbb{Q}}$. A calculation of these symbols shows that this condition is in turn equivalent to the condition $(\gamma, m)_p = +1$ for all $p \in \Omega_{\mathbb{Q}}$.

(iii) $\Leftrightarrow$ (iv) These conditions are equivalent because $(\gamma, m)_p = 1$ for all odd p that do not divide either m or γ. QED

For the purpose of the present problem, we consider those elements satisfying the conditions (**) where the set $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_s$ varies through all possible subsets of the set $\mathscr{M}(\tilde{L})$. For each of these subsets obtain one element of E satisfying these conditions (if such an element does in fact exist); let $\alpha_1, \ldots, \alpha_u$ be a list of these elements. Always choose α_i to have $N_{E/\mathbb{Q}}(\alpha_i) > 0$ whenever possible and arrange the elements in such a way that $N_{E/\mathbb{Q}}(\alpha_i) > 0$ for $i = 1, \ldots, u'$ and $N_{E/\mathbb{Q}}(\alpha_i) < 0$ if $i = u' + 1, \ldots, u$ (of course, $u' = u$ if $m > 0$ with $N_{E/\mathbb{Q}}(\varepsilon) = -1$ or if $m < 0$). Our discussion can be summarized in the following theorem. Recall that $p_1, \ldots, p_t$ denote those rational primes that divide $\mathrm{disc}(E/\mathbb{Q})$.

Theorem 1.7 *Let L be a $\mathbb{Z}$-lattice with $\dim L \geq 3$ and L_2 modular. Let $\bar{j} \neq \bar{1} \in \mathscr{G}_{\mathbb{Q}}(L)$. $\psi_L(\bar{j}) = \bar{1} \in \mathscr{G}_E(\tilde{L})$ if and only if there exists $\alpha \in \dot{E}$ for which $(\alpha)h(j) \in J_E^{\tilde{L}}$ and:*

(i) *If L is definite, $m > 0$ and $N_{E/\mathbb{Q}}(\varepsilon) = +1$, α is a product of elements from the list $1, \varepsilon, p_1, \ldots, p_t, \alpha_1, \ldots, \alpha_{u'}$.*

(ii) *If L is definite, $m > 0$ and $N_{E/\mathbb{Q}}(\varepsilon) = -1$, α is a product of elements from the list* $1, p_1, \ldots, p_t, \alpha_1, \ldots, \alpha_{u'}$.

(iii) *If $m < 0$ or if L is indefinite, α is a product of the elements* $1, \varepsilon, p_1, \ldots, p_t, \alpha_1, \ldots, \alpha_u$.

Example 1.8 Consider the lattice L of Example 1.2. The map ψ_L is injective if and only if $\psi_L(\bar{j})$ is a nontrivial element of $\mathscr{G}_E(\tilde{L})$. We consider several extensions E.

(i) $E = \mathbb{Q}(\sqrt{3})$. We have $\psi_L(\bar{j}) = (\bar{2})\psi_L(\bar{j}) = \psi_L(\bar{k})$. Furthermore, $\Delta_{19} \in \dot{E}_{\mathfrak{p}}^2$ for $\mathfrak{p} = 19\mathfrak{o}$, since 19 is inert in $E/\mathbb{Q}$. Thus, $\psi_L(\bar{k}) = (\bar{1})$ and ψ_L is not injective.

(ii) $E = \mathbb{Q}(\sqrt{5})$. Since 3 is inert in $E/\mathbb{Q}$, we have $\Delta_3 \in \dot{E}_{\mathfrak{p}}^2$ for $\mathfrak{p} = 3\mathfrak{o}$ and $\psi_L(\bar{j}) = (\bar{1})$; again ψ_L is not injective.

(iii) $E = \mathbb{Q}(\sqrt{7})$. According to Theorem 1.7 we need only check the multiples of $\psi_L(\bar{j})$ by products of the elements 1, 2, 7, ε, and β where $\varepsilon = 8 + 3\sqrt{7}$ and $N_{E/\mathbb{Q}}(\beta) = 2$. First consider ε. Since $\sqrt{7} = \pm 1$ in $\bar{\mathbb{Q}}_3 \cong \mathbb{Z}/(3)$ and $\sqrt{7} = \pm 8$ in $\bar{\mathbb{Q}}_{19} \cong \mathbb{Z}/(19)$, ε is seen to be a nonsquare at each of the spots lying above 3 and 19. So $(\bar{\varepsilon})\psi_L(\bar{j}) \neq (\bar{1})$. We may choose $\beta = 3 + \sqrt{7}$. Local calculation shows that β is a square at one spot lying over 3 and a nonsquare at the other. Thus, $(\bar{\beta})\psi_L(\bar{j}) \neq (\bar{1})$. Hence, $\psi_L(\bar{j}) \neq (\bar{1})$ and ψ_L is injective.

2. Spinor Norms in Quadratic Fields

The problem of computing the spinor norms of local integral rotations on a lattice K at the spots $\mathfrak{p}$ of $\mathbb{Q}(\sqrt{m})$ has been completely solved (see Kneser [11] and Earnest and Hsia [5]) unless $\mathfrak{p}$ is a ramified dyadic spot; i.e., $\mathfrak{p} \mid 2$ and $e(\mathfrak{p} \mid 2) = 2$. In this section we calculate these spinor norm groups for the particular case of such localizations of a lattice $\tilde{L}$ lifted from $\mathbb{Q}$. Since 2 ramifies in $\mathbb{Q}(\sqrt{m})$, m must be congruent to 2 or 3 modulo 4, and the results here vary significantly depending upon the specific congruence. The computations depend strongly upon the fact that the residue class field of $\mathbb{Q}(\sqrt{m})$ at $\mathfrak{p}$ contains only two elements; in particular, any sum of two units of $\mathbb{Q}(\sqrt{m})_{\mathfrak{p}}$ lies in the ideal $\mathfrak{p}$.

In this section, we adapt our notation to this purely local situation. A dyadic prime spot on $\mathbb{Q}(\sqrt{m})$, $m \equiv 2$ or 3 (mod 4), is denoted by $\mathfrak{p}$ and F is the completion of $\mathbb{Q}(\sqrt{m})$ at $\mathfrak{p}$. L will be a lattice over $\mathbb{Z}_2$, the integers of $\mathbb{Q}_2$, and so $\tilde{L}$ is a lattice over $\mathfrak{o}$, the ring of integers of F. Since the spinor norm groups are unaffected by scaling, we shall assume $sL = \mathbb{Z}_2 \cdot u_2$ and $u_{\mathfrak{p}}$ are the groups of units of $\mathbb{Z}_2$ and $\mathfrak{o}$, respectively. Finally, π denotes a fixed prime in F; i.e., $\pi\mathfrak{o} = \mathfrak{p}$. Then $2 = \pi^2\beta$ for some $\beta \in \mathfrak{o}$. In the following proposition, which makes clear the local distinction of the cases $m \equiv 2$ or 3 (mod 4), we

describe a choice of the element π and examine the resulting β. The symbol $\mathscr{D}$ denotes the quadratic defect as described in O'Meara [12].

Proposition 2.1 $\mathscr{D}(2) = \mathfrak{p}^3 \Leftrightarrow m \equiv 3 \pmod 4$.

Proof If $m \equiv 2 \pmod 4$, write $m = 2m'$, m' an odd integer. Let $\pi = \sqrt{m/m'}$. Then $\pi^2 = m/m'^2 = 2m'/m'^2 = 2/m'$. So, $2 = \pi^2 m'$; that is, $\beta = m' \in \mathfrak{u}_2$, so $\mathscr{D}(\beta) \subseteq \mathfrak{p}^3$. Hence, $\mathscr{D}(2) \subseteq \mathfrak{p}^5$ and it follows that $\mathscr{D}(2) = 0$.

Conversely, if $m \equiv 3 \pmod 4$, then write $m = 3 + 4t$ and let $\alpha = 2 + 2t - \sqrt{m}$. This $\alpha \in \mathfrak{o}$ and a direct calculation shows $N_{F/Q_2}(\alpha) \in \mathfrak{u}_2$ and it follows that $\alpha \in \mathfrak{u}_\mathfrak{p}$. Choose $\pi = (\sqrt{m} - 1)/\alpha$. Then $2 = \pi^2\alpha$. Furthermore, $\alpha = 1 + (1 + 2t + \sqrt{m})$ and $N_{F/Q_2}(1 + 2t + \sqrt{m})$ is a prime element of $\mathbb{Z}_2$, so $1 + 2t + \sqrt{m}$ is a prime element of $\mathfrak{o}$. In this case, $\mathscr{D}(\alpha) = \mathfrak{p}$ and $2 = \pi^2\alpha$ gives $\mathscr{D}(2) = \mathfrak{p}^3$. QED

The next proposition reduces the problem of calculating spinor norms of all elements of $O^+(\tilde{L})$ to that of performing the calculations only for the symmetries in $O(\tilde{L})$.

Proposition 2.2 *$O(\tilde{L})$ is generated by the symmetries S_x and Eichler transformations E^i_w in $O(\tilde{L})$.*

Proof Apply induction on dim L. It suffices to consider those L with $sL = \mathbb{Z}_2$. For such a lattice, $L = L_1 \perp M$ with L_1 unimodular and $sM \subseteq 2\mathbb{Z}_2$. If L_1 is split by a hyperbolic plane the result follows as in O'Meara and Pollak [13, 14]. Since the orders of norm and weight generators of $\tilde{L}_1$ are both even, $\tilde{L}_1$ is split in that way whenever dim $L_1 \geq 3$. So we need only consider dim $L_1 \leq 2$. Furthermore, if $L_1 \cong A(2, 2)$ or L_1 unary, the result follows as in proof of Proposition 2.1 of Earnest and Hsia [7].

Suppose $L_1 \cong A(\varepsilon, 2\delta)$, with $\varepsilon, \delta \in \mathfrak{u}_2$, in basis $\{x, y\}$ and $\sigma \in O(\tilde{L})$. Then at least one of the symmetries $S_{\sigma(x)-x}$ or $S_{S_y\sigma(x)-x}$ lies in $O(\tilde{L})$ and the result follows by induction since $\mathfrak{o}x$ splits $\tilde{L}$ and there is a z with $S_z \in O(\tilde{L})$ for which $S_z\sigma$ or $S_zS_y\sigma$ fixes x. If $L_1 \cong A(1, 0)$ or $A(1, 4)$ in basis $\{x, y\}$, then one of $S_{\sigma(x)-x}$ or $S_{S_{\pi x+y}\sigma(x)-x}$ lies in $O(\tilde{L})$ and the result follows similarly. This exhausts all possibilities. QED

We need one further calculation in order to simplify the statements of later results.

Lemma 2.3 *Let $d \in \mathfrak{u}_2$. Then the F-space $[1, d]$ represents all units h that lie in $1 + \mathfrak{p}^2$.*

Proof The quadratic defect $\mathscr{D}(-d)$ is contained in $\mathfrak{p}^3$. If $\mathscr{D}(-d) \subseteq 4\mathfrak{o}$, then the result follows since the Hilbert symbol $(h, -d)_\mathfrak{p} = +1$ for any $h \in \mathfrak{u}_\mathfrak{p}$. So we treat the case $\mathscr{D}(-d) = \mathfrak{p}^3$. Write $-d = 1 + \pi^3\varepsilon$, $\varepsilon \in \mathfrak{u}_\mathfrak{p}$. A

basis $\{x, y\}$ for the space can be chosen for which the corresponding matrix is

$$\begin{pmatrix} 1 & 1 \\ 1 & -\pi^3\varepsilon \end{pmatrix}.$$

We shall show there is a vector $v = x + Cy$ with $C \in F$ for which $Q(v) = h$. By perfectness of the residue class field, h can be written as $h = 1 + 2r$, $r \in \mathfrak{p}$. Now $Q(v) = 1 + 2C - \pi^3\varepsilon C^2 = 1 + 2(C + \pi\varepsilon' C^2)$, $\varepsilon' \in \mathfrak{u}_\mathfrak{p}$. The polynomial $f(X) = \pi\varepsilon' X^2 + X - r$ is reducible by the reducibility criterion of 13 : 9 [12]. That is, $f(X)$ has a linear factor, and thus a root in F. Taking C equal to this root gives the desired vector. QED

We now proceed with specific calculation of the spinor norm groups. These groups were computed in Hsia [9] for modular lattices with no restrictions on the nature of the local field. From results obtained there, it can be seen that $\theta(O^+(\tilde{L})) = \mathfrak{u}_\mathfrak{p}\dot{F}^2$ whenever $\dim L \geq 2$ and L modular but $L \ncong A(\varepsilon, 2\delta)$ where $\varepsilon, \delta \in \mathfrak{u}_2$. Proposition E of Hsia [9] applies to this exceptional case, but does not yield a solution in closed form. However, in the present context the situation is seen to be considerably simpler.

Proposition 2.4 *Let* $L \cong A(1, 2\gamma)$, $\gamma \in \mathfrak{u}_2$.

(i) *If* $m \equiv 2 \pmod 4$, *then* $\theta(O^+(\tilde{L})) = (1 + \mathfrak{p}^2)\dot{F}^2$.
(ii) *If* $m \equiv 3 \pmod 4$, *then* $\theta(O^+(\tilde{L})) = \mathfrak{u}_\mathfrak{p}\dot{F}^2$.

Proof We first show that $(1 + \mathfrak{p}^2)\dot{F}^2 \subseteq \theta(O^+(\tilde{L}))$ in any case. The lattice L can be rewritten over $\mathbb{Z}_2$ as $L \cong \langle 1\rangle \perp \langle d\rangle$, $d = \det L \in \mathfrak{u}_2$. Let $h = 1 + 2\tau$, $\tau \in \mathfrak{o}_\mathfrak{p}$. Then $g\langle h, h^{-1}d\rangle = h\mathfrak{o}_\mathfrak{p}^2 + 2\mathfrak{o}_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}^2 + 2\mathfrak{o}_\mathfrak{p} = g\langle 1, d\rangle$ and the spaces $[h, h^{-1}d]$ and $[1, d]$ are isometric over F by Lemma 2.3, so $\langle h, h^{-1}d\rangle$ and $\langle 1, d\rangle$ are isometric over $\mathfrak{o}$ by 93 : 16 of [12]. In particular, $\langle 1, d\rangle$ represents h over $\mathfrak{o}$. Since $h \in \mathfrak{u}_\mathfrak{p}$, the vector of $\tilde{L}$ of length h gives rise to a symmetry of $\tilde{L}$.

Next, suppose $v = Ax + Cy \in P(\tilde{L})$, where $\{x, y\}$ is a basis adapted to $A(1, 2\gamma)$. Further, write $2\gamma = \pi^2 f$ noting that $f \in \mathfrak{u}_2$ when $m \equiv 2 \pmod 4$ and $\mathscr{D}(f) = \mathfrak{p}$ when $m \equiv 3 \pmod 4$. If $A \in \mathfrak{u}_\mathfrak{p}$, $Q(v)$ is clearly an element of $(1 + \mathfrak{p}^2)\mathfrak{u}_\mathfrak{p}^2$. So assume $A \in \mathfrak{p}$ and, without loss of generality, $C = 1$. Thus, $Q(v) = A^2 + \pi^2 f$. If $\operatorname{ord}_\mathfrak{p} A = 1$, then $Q(v) \in \mathfrak{p}^3$; but $B(v, x) \in \mathfrak{u}_\mathfrak{p}$. So no such v can give rise to an integral symmetry. If $\operatorname{ord}_\mathfrak{p} A \geq 2$, it is clear that $\operatorname{ord}_\mathfrak{p} Q(v) = \operatorname{ord}_\mathfrak{p}(\pi^2 f) = 2$ and, thus, we get $\theta(O^+(\tilde{L})) \subseteq \mathfrak{u}_\mathfrak{p}\dot{F}^2$. In the case $m \equiv 2 \pmod 4$, this containment can be strengthened because $Q(v) = A^2 + \pi^2 f = \pi^2 f(1 + A^2\pi^{-2}f^{-1})$ and $\operatorname{ord}_\mathfrak{p} A \geq 2$ shows that

$$1 + A^2\pi^{-2}f^{-1} \in 1 + \mathfrak{p}^2,$$

but furthermore, $f \in 1 + \mathfrak{p}^2$ since $f \in \mathfrak{u}_2$. So $Q(v) \in (1 + \mathfrak{p}^2)\mathfrak{u}_\mathfrak{p}^2$ and we obtain the reverse containment, $(1 + \mathfrak{p}^2)\dot{F}^2 \supseteq \theta(O^+(\tilde{L}))$. However, when

$m \equiv 3 \pmod 4$, $Q(v) \notin (1 + \mathfrak{p}^2)\dot{F}^2$ for the vector $v = 2x + y \in P(\tilde{L})$. So in that case, $\theta(O^+(\tilde{L})) = \mathfrak{u}_\mathfrak{p}\dot{F}^2$. QED

Remark 2.5 In the present context, $1 + \mathfrak{p}^2 = \mathfrak{u}_\mathfrak{p}^2(1 + \mathfrak{p}^2)$ is a subgroup of $\mathfrak{u}_\mathfrak{p}$ of index two.

Hence we see that the spinor norm group $\theta(O^+(\tilde{L}))$ has a very convenient form when L is modular. To compute the general nonmodular case, we will be able to determine the spinor norms using the components of a Jordan splitting and sublattices of the form $\langle 1\rangle \perp \langle 2^r\gamma\rangle, r \geq 1$ and $\gamma \in \mathfrak{u}_2$. We now turn our attention to these binary nonmodular lattices.

Proposition 2.6 *Let* $m \equiv 2 \pmod 4$ *and* $L \cong \langle 1, 2\gamma\rangle$, $\gamma \in \mathfrak{u}_2$. *Then* $\theta(O^+(\tilde{L})) = (1 + \mathfrak{p}^2)\dot{F}^2$.

Proof Let $\{x, y\}$ be a basis for $\langle 1, 2\gamma\rangle$. Write $2\gamma = \pi^2 f$ where, since $m \equiv 2 \pmod 4$, f can be chosen from $\mathfrak{u}_2$. In particular, $f = 1 + 2g$, $g \in \mathfrak{u}_2$.

To show the containment $\subseteq$, take $v = Ax + Cy \in P(\tilde{L})$, $A, C \in \mathfrak{o}$. If $A \in \mathfrak{u}_\mathfrak{p}$, $C \in \mathfrak{p}$ it is clear that $Q(v) \in (1 + \mathfrak{p}^2)\dot{F}^2$. If both $A \in \mathfrak{u}_\mathfrak{p}$ and $C \in \mathfrak{u}_\mathfrak{p}$, assume $A = 1$ and write $Q(v) = 1 + \pi^2C^2f = 1 + \pi^2C^2 + 2\pi^2C^2g = (1 + \pi C)^2 + 2\pi^2C^2g - 2\pi C \in (1 + \mathfrak{p}^2)F^2$. When $A \in \mathfrak{p}$, assume $C = 1$; then if $\operatorname{ord}_\mathfrak{p} A \geq 2$, $Q(v) = \pi^2 f(1 + A^2\pi^{-2}f^{-1}) \in (1 + \mathfrak{p}^2)\dot{F}^2$ since $f \in 1 + \mathfrak{p}^2$. The case $C = 1$, $\operatorname{ord}_\mathfrak{p} A = 1$ does not give a symmetry in $O(\tilde{L})$. This exhausts all possibilities.

Conversely, if $h \in 1 + \mathfrak{p}^2$, then $\langle 1, f\rangle \cong \langle h, h^{-1}f\rangle$ by Lemma 2.3 and 93 : 16 [12]. So there are $s, t \in \mathfrak{o}$ for which $h = s^2 + t^2 f$. If $t \in \mathfrak{u}_\mathfrak{p}$ the vector $v = \pi sx + ty$ of $\tilde{L}$ has length $\pi^2 h$. If $t \in \mathfrak{p}$, the vector $v = sx + t\pi^{-1}y$ has length h. QED

Proposition 2.7 *Let* $m \equiv 3 \pmod 4$ *and* $L \cong \langle 1, 2\gamma\rangle$, $\gamma \in \mathfrak{u}_2$. *Then* $\theta(O^+(\tilde{L})) = \{\eta \in F\colon (\eta, -f)_\mathfrak{p} = +1\}$ *where* $2\gamma = \pi^2 f$.

Proof Consider the lattice $\mathscr{L} \cong \langle 1, f\rangle$ over $\mathfrak{o}$ in basis $\{x, w\}$. The lattice with basis $\{x, \pi w\}$ is isometric to $\tilde{L}$, so we may view $\tilde{L}$ as a sublattice of $\mathscr{L}$. In particular, $\theta(O^+(\tilde{L})) \subseteq \theta(O^+(\mathscr{L}))$. Conversely, suppose

$$v = Ax + Cw \in P(\mathscr{L}).$$

If $A \in \mathfrak{u}_\mathfrak{p}$, $C \in \mathfrak{p}$, say $C = \pi\zeta$, then $u = Ax + \zeta y \in P(\tilde{L})$ with $Q(u) = Q(v)$. If $C \in \mathfrak{u}_\mathfrak{p}$, assume $C = 1$ and consider the vector $u = A\pi x + y \in \tilde{L}$. Then $Q(u) = \pi^2 Q(v)$ and it remains only to verify that $S_u \in O(\tilde{L})$. When $A \in \mathfrak{p}$, $Q(u) \in 2\mathfrak{u}_\mathfrak{p}$ and $S_u \in O(\tilde{L})$. If $A \in \mathfrak{u}_\mathfrak{p}$, then we observe that $\mathscr{D}(f) = \mathfrak{p}$ since $m \equiv 3 \pmod 4$ and that $|Q(v)| = |A^2 + f| = |\pi|$. Furthermore, $2B(u, \tilde{L}) = \mathfrak{p}^3 = Q(u)\mathfrak{o}$ and $S_u \in O(\tilde{L})$ in this case also. Thus, we have shown that $\theta(O^+(\tilde{L})) = \theta(O^+(\mathscr{L}))$. But the group on the right can be determined by Proposition B of Hsia [9] and is seen to equal the set of elements satisfying the Hilbert symbol $(\eta, -f)_\mathfrak{p} = +1$. QED

Remark 2.8 In the case described by the above proposition, $\theta(O^+(\tilde{L}))$ has index two in F. This is the first instance in which we do not have $\theta(O^+(\tilde{L})) \subseteq \mathfrak{u}_\mathfrak{p}\dot{F}^2$. It will be seen (Lemma 2.19) that this is the only way in which this containment can be violated.

The calculation of $\theta(O^+(\tilde{L}))$ when $L = \langle 1, 4\gamma\rangle$, $\gamma \in \mathfrak{u}_2$ has been done in Proposition 3.1 of [7]. Here there is no distinction between $m \equiv 2$ or 3 (mod 4) and, combining this result with Lemma 2.3, we obtain:

Proposition 2.9 *Let* $L = \langle 1, 4\gamma\rangle$, $\gamma \in \mathfrak{u}_2$. *Then* $\theta(O^+(\tilde{L})) = (1 + \mathfrak{p}^2)\dot{F}^2$.

Additionally, the cases $L = \langle 1, 2^r\gamma\rangle$, $\gamma \in \mathfrak{u}_2$, $r \geq 4$ are determined by 3.3 and 3.4 of [7]. So the binary cases will be completely resolved with the calculation of $\theta(O^+(\tilde{L}))$ for $L \cong \langle 1, 8\gamma\rangle$. Again in this case, we treat separately $m \equiv 2 \pmod 4$ and $m \equiv 3 \pmod 4$. In either case, if $\{x, y\}$ is a basis for the given splitting and $v = Ax + Cy \in P(L)$, restrictions on the possible values of A and C are given by Proposition 3.2 of [7]. From these restrictions, it can be easily seen that $\theta(O^+(\tilde{L})) \subseteq \mathfrak{u}_\mathfrak{p}\dot{F}^2$.

Proposition 2.10 *Let* $m \equiv 2 \pmod 4$ *and* $L \cong \langle 1, 8\gamma\rangle$. *Then* $\theta(O^+(\tilde{L})) = (1 + \mathfrak{p}^2)\dot{F}^2$.

Proof It is easy to see that $(1 + \mathfrak{p}^4)\dot{F}^2 \subseteq \theta(O^+(\tilde{L})) \subseteq (1 + \mathfrak{p}^2)\dot{F}^2$ by using Proposition 3.2 [7]. So it will suffice to show that for any $\tau = 1 + 2\pi\varepsilon$ with $\varepsilon \in \mathfrak{u}_\mathfrak{p}$, there is $v \in P(\tilde{L})$ with $Q(v) \in \tau\dot{F}^2$. We shall show there is such a $v = Ax + Cy$ with $C \in \mathfrak{u}_\mathfrak{p}$ and $A = 2\alpha$, $\alpha \in \mathfrak{u}_\mathfrak{p}$.

Since $m \equiv 2 \pmod 4$ we can write $8\gamma = 4\pi^2 f$ where $f \in \mathfrak{u}_2$. In particular, $-f \in 1 + \mathfrak{p}^3$ and $C^2 \in 1 + \mathfrak{p}^2$ gives $-C^2\pi^2 f = \pi^2(1 + 2s)$ for some $s \in \mathfrak{o}$. Consider

$$\tau - C^2\pi^2 f = 1 + 2\pi\varepsilon - C^2\pi^2 f = (1 + \pi)^2\left[1 + \frac{2\pi((\varepsilon - 1) + \pi s)}{(1 + \pi)^2}\right].$$

If $\varepsilon \notin 1 + \mathfrak{p}^2$, then by taking $C = 1 + \pi$ we see that $s \in \mathfrak{u}_\mathfrak{p}$ and the expression in square brackets is of the form $1 + 4\pi\eta$, $\eta \in \mathfrak{o}$ and is thus a square by the local square theorem; say $(1 + \pi)^2(1 + 4\pi\eta) = \alpha^2$, $\alpha \in \mathfrak{u}_\mathfrak{p}$. Then the vector $v = 2\alpha x + (1 + \pi)y$ has length $Q(v) = 4\alpha^2 + (1 + \pi^2)4\pi^2 f = 4(\alpha^2 + (1 + \pi^2)f\pi^2) = 4(\tau - (1 + \pi)^2\pi^2 f + (1 + \pi)^2\pi^2 f) = 4\tau \in \tau\dot{F}^2$. On the other hand, if $\varepsilon \in 1 + \mathfrak{p}^2$, then taking $C = 1$ gives $s \in \mathfrak{p}$ and again the expression in square brackets is a square; say $\alpha^2 = (1 + \pi)^2(1 + 4\pi\eta)$ again. This time $v = 2\alpha x + y$ is the desired vector. QED

Proposition 2.11 *Let* $m \equiv 3 \pmod 4$ *and* $L \cong \langle 1, 8\gamma\rangle$, $\gamma \in \mathfrak{u}_2$. *Then* $\theta(O^+(\tilde{L})) = \{\eta \in \mathfrak{u}_\mathfrak{p}: (\eta, -f)_\mathfrak{p} = +1\}\dot{F}^2$ *where* $8\gamma = 4\pi^2 f$.

Proof We again view $\tilde{L}$ as a sublattice of $\mathscr{L} = \langle 1, f \rangle \leftrightarrow \{x, w\}$, $y = 2\pi w$. It suffices to show that $\theta(O^+(\tilde{L})) = (\mathfrak{u}_\mathfrak{p} \cap Q(P(\mathscr{L})))\dot{F}^2$. Let $u = Ax + Cy \in P(\tilde{L})$. If $A \in \mathfrak{u}_\mathfrak{p}$, then $Q(u) \in \dot{F}^2$. If $C \in \mathfrak{u}_\mathfrak{p}$ we may take $C = 1$ and restrictions on the value of A are given by 3.2 of [7]. For $0 < \operatorname{ord}_\mathfrak{p} A \leq 2$, the vector $v = x + 2\pi A^{-1}w$ lies in $P(\mathscr{L})$ and has length $A^{-2}A(u)$. For $\operatorname{ord}_\mathfrak{p} A \geq 4$, the vector $v = (A/2\pi)x + w$ lies in $P(\mathscr{L})$ and has length $(1/2\pi)^2 Q(u)$. This shows $\theta(O^+(\tilde{L})) \subseteq (\mathfrak{u}_\mathfrak{p} \cup Q(P(\mathscr{L})))\dot{F}^2$.

Conversely, let $v = Ax + Cw \in P(\mathscr{L})$, $Q(v) \in \mathfrak{u}_\mathfrak{p}$. If $C \in \mathfrak{p}^3$, write $C = 2\pi C_0$, $C_0 \in \mathfrak{o}_\mathfrak{p}$, and consider the vector $u = Ax + C_0 y$. This vector has length $Q(v)$ and lies in $P(\tilde{L})$. If $0 < \operatorname{ord}_\mathfrak{p} C \leq 2$, then $2\pi C^{-1} \in \mathfrak{u}_\mathfrak{p}$ and $v = 2\pi C^{-1}x + y \in P(\tilde{L})$ has length $Q(u) = (2\pi C^{-1})^2 Q(v)$. So we are left with $C \in \mathfrak{u}_\mathfrak{p}$; take $C = 1$. The vector $u = 2\pi Ax + y$ has length $Q(u) = (2\pi)^2 \times (A^2 + f) = (2\pi)^2 Q(v)$. When $A \in \mathfrak{p}$, $2\pi A \in \mathfrak{p}^4$ and so $u \in P(\tilde{L})$. Finally, if $A \in \mathfrak{u}_\mathfrak{p}$, then $|Q(v)| = |\pi|$ since $\mathscr{D}(f) = \mathfrak{p}$, and $Q(v)$ does not lie in $Q(P(\mathscr{L})) \cap \mathfrak{u}_\mathfrak{p})\dot{F}^2$. QED

We turn now to the question of determining $\theta(O^+(\tilde{L}))$ for a general L by considering a Jordan splitting of L. The results vary markedly depending upon the congruence of m mod 4. We treat first the case $m \equiv 2 \pmod 4$. In this case, we have observed for binary L that $\theta(O^+(\tilde{L})) \subseteq \mathfrak{u}_\mathfrak{p}\dot{F}^2$. This result can be extended to lattices of arbitrary dimension by an inductive argument and a consideration of all possibilities for the structure of the first Jordan component of a splitting of the given lattice. The result is stated here without proof.

Lemma 2.12 *If $m \equiv 2 \pmod 4$, then $\theta(O^+(\tilde{L})) \subseteq \mathfrak{u}_\mathfrak{p}\dot{F}^2$.*

This lemma has several immediate consequences.

Theorem 2.13 *Let $m \equiv 2 \pmod 4$.*

(i) *If L has a Jordan component of dimension 3 or more, then $\theta(O^+(\tilde{L})) = \mathfrak{u}_\mathfrak{p}\dot{F}^2$.*

(ii) *If L has a binary Jordan component which is not of the form $2^r A(\varepsilon, 2\delta)$, $r \in \mathbb{N} \cup \{0\}$, $\varepsilon, \delta \in \mathfrak{u}_2$, then $\theta(O^+(\tilde{L})) = \mathfrak{u}_\mathfrak{p}\dot{F}^2$.*

So we may now assume that L has a Jordan splitting $L = L_1 \perp 2^{r_2}L_2 \perp \cdots \perp 2^{r_t}L_t$ with $\dim L_i \leq 2$ and all binary L_i have the form $A(\varepsilon, 2\delta)$, $\varepsilon, \delta \in \mathfrak{u}_2$.

We first treat the case when all L_i are unary.

Theorem 2.14 *Let $m \equiv 2 \pmod 4$,*

$$L = \mathbb{Z}_2 x_1 \perp \cdots \perp \mathbb{Z}_2 x_t = \langle 2^{r_1}\varepsilon_1 \rangle \perp \langle 2^{r_2}\varepsilon_2 \rangle \perp \cdots \perp \langle 2^{r_t}\varepsilon_t \rangle$$

be a Jordan splitting of L. Then

$$\theta(O^+(\tilde{L})) = \left\{ \prod^{\text{even}} Q(v) \colon v \in P(\mathfrak{o}x_j \perp \mathfrak{o}x_{j+1}),\ 1 \leq j \leq t-1 \right\}.$$

Proof This result has already been obtained in 3.8 [7] unless there are indices k, s, and t for which $r_{k+1} - r_k = 1$ or 3 and $r_s - r_t = 2$ or 4. For such lattices we have established that

$$\theta(O^+(\tilde{L})) \supseteq (1 + \mathfrak{p}^2)\dot{F}^2 = \theta(O^+(\mathfrak{o}x_k + \mathfrak{o}x_{k+1})).$$

So it suffices to show that $\theta(O^+(\tilde{L})) = (1 + \mathfrak{p}^2)\dot{F}^2$. For any vector $v = \sum_{i=1}^{t} A_i x_i \in P(\tilde{L})$, the condition $m \equiv 2 \pmod 4$ assures that there is exactly one index $i = i_0$ for which $A_i^2 Q(x_i)$ has maximal value. But since each $A_i^2 Q(x_i)$ has even order, it follows that

$$Q(v) = Q(A_{i_0} X_{i_0}) + \sum_{i \neq i_0} Q(A_i X_i) \in Q(A_{i_0} X_{i_0})(1 + \mathfrak{p}^2)$$

$$\subseteq (1 + \mathfrak{p}^2) \subseteq (1 + \mathfrak{p}^2)\dot{F}^2. \quad \text{QED}$$

We now treat the case when there is at least one binary component and all binary L_i have the form $A(\varepsilon, 2\delta)$, $\varepsilon, \delta \in \mathfrak{u}_2$. By Proposition 2.4, $\theta(O^+(\tilde{L}))$ contains the subgroup $(1 + \mathfrak{p}^2)\dot{F}^2$ of index two in $\mathfrak{u}_\mathfrak{p}\dot{F}^2$; thus, $\theta(O^+(\tilde{L}))$ must equal either $(1 + \mathfrak{p}^2)\dot{F}^2$ or $\mathfrak{u}_\mathfrak{p}\dot{F}^2$. If the components are not too closely bunched, only $(1 + \mathfrak{p}^2)\dot{F}^2$ is attained.

Theorem 2.15 *Assume that $m \equiv 2 \pmod 4$ and L has a Jordan splitting of the type described above. Then $\theta(O^+(\tilde{L})) = (1 + \mathfrak{p}^2)\dot{F}^2$ unless L is split by a sublattice $2^r K$ of the form $K = \langle \varepsilon \rangle \perp 2A(\eta, 2\mu)$ or $K = A(\eta, 2\mu) \perp 2\langle \varepsilon \rangle$. In this case, $\theta(O^+(\tilde{L})) = \mathfrak{u}_\mathfrak{p}\dot{F}^2$.*

Proof Suppose L contains a sublattice $2^r K$ of one of the given types in basis $\{x, y, z\}$. If $K = \langle \varepsilon \rangle \perp 2A(\eta, 2\mu)$ the vector $v = 2x + \pi y + z \in P(\tilde{K})$ has $Q(v) \notin (1 + \mathfrak{p}^2)\dot{F}^2$. Since $\theta(O^+(A(\eta, 2\mu))) = (1 + \mathfrak{p}^2)\dot{F}^2$ has index two in $\mathfrak{u}_\mathfrak{p}\dot{F}^2$, $\theta(O^+(\tilde{L}))$ must be all of $\mathfrak{u}_\mathfrak{p}\dot{F}^2$.

To show that in all other cases $\theta(O^+(\tilde{L})) = (1 + \mathfrak{p}^2)\dot{F}^2$, apply induction on the number of Jordan components making use of the following lemma:

Lemma 2.16 *Suppose $L = K \perp M$ where $K = A(\eta, 2\mu)$ or $K = \langle \varepsilon \rangle$ and $M \subseteq 4\mathbb{Z}_2$. If $\theta(O^+(\tilde{M})) \subseteq (1 + \mathfrak{p}^2)\dot{F}^2$, then $\theta(O^+(\tilde{L})) \subseteq (1 + \mathfrak{p}^2)\dot{F}^2$.*

Proof We shall write only the case $K = A(\eta, 2\mu)$ since the argument for $K = \langle \varepsilon \rangle$ is contained therein. For any $v \in P(\tilde{L})$, write $v = Ax + Cy + z$ where $\{x, y\}$ is a basis for K, $A, C \in \mathfrak{o}$ and $z \in \tilde{M}$. If $\operatorname{ord}_\mathfrak{p} A \leq 1$, then $Q(z) \in Q(Ax + Cy)(1 + \mathfrak{p}^2)$. When $\operatorname{ord}_\mathfrak{p} A \geq 2$, $v \in P(\tilde{L})$ forces either $C \in \mathfrak{u}_\mathfrak{p}$ or both A and C lie in $\mathfrak{p}^3$. In the latter case, if $Q(z) \in 4\mathfrak{u}_\mathfrak{p}$, then $Q(Ax + Cy) \in Q(z)(1 + \mathfrak{p}^2)$. We are left with the case $Q(z) \in 8\mathfrak{o}$ and $|Q(v)| = |Q(z)|$. If $\operatorname{ord}_\mathfrak{p} Q(z) = t$, the condition $v \in P(\tilde{L})$ gives $A, C \in \mathfrak{p}^{t-2}$. So A^2, C^2, and AC all lie inside $\mathfrak{p}^{2t-4}$ and, since $t \geq 6$, we have $2t - 4 \geq t + 2$. Thus, $Q(v) \in Q(z)(1 + \mathfrak{p}^2)$. This exhausts all possibilities and the lemma is proved. QED

We now complete the case $m \equiv 3 \pmod 4$. The Theorem 2.14 remains true also in this case.

Theorem 2.17 *Let* $m \equiv 3 \pmod 4$ *and let* $L = \mathbb{Z}_2 x_1 \perp \cdots \perp \mathbb{Z}_2 x_t = \langle 2^{r_1}\varepsilon_1 \rangle \perp \cdots \perp \langle 2^{r_t}\varepsilon_t \rangle$ *be a Jordan splitting of* L. *Then*

$$\theta(O^+(\tilde{L})) = \left\{ \prod^{\text{even}} Q(v) \colon v \in P(\mathfrak{o}x_j \perp \mathfrak{o}x_{j+1}),\ 1 \le j \le t-1 \right\}.$$

Proof The result follows from Theorem 3.8 of Earnest and Hsia [7] unless there are indices k, s, and t for which $r_{k+1} - r_k = 1$ or 3 and $r_s - r_t = 2$ or 4. If $r_{k+1} - r_k = 1$ and $r_s - r_t = 2$, then $\theta(O^+(\tilde{L})) = \dot{F}$ because $\theta(O^+(\mathfrak{o}x_s \perp \mathfrak{o}x_t)) = (1 + \mathfrak{p}^2)\dot{F}^2 \not\subseteq \theta(O^+(\mathfrak{o}x_k \perp \mathfrak{o}x_{k+1}))$. This follows from the duality lemma of Ankeny and Hsia [1] which shows that for $-f$ with $\mathscr{D}(-f) = \mathfrak{p}$ there is an element μ with $\mathscr{D}(\mu) = \mathfrak{p}^3$ for which $(\mu, -f)_{\mathfrak{p}} = -1$. So we may assume there are no such indices.

For a vector $v = \sum_{i=1}^{t} A_i X_i \in P(\tilde{L})$, let k be the largest index for which $\operatorname{ord}_{\mathfrak{p}} Q(A_k X_k)$ is minimal. If there is another $j < k$ with $\operatorname{ord}_{\mathfrak{p}} Q(A_k X_k) = \operatorname{ord}_{\mathfrak{p}} Q(A_j X_j)$, it follows easily that $j = k-1$, $r_j = r_k - 1$, $A_k \in \mathfrak{u}_{\mathfrak{p}}$, and $|A_j| = |\pi|$. Since $r_s - r_t \neq 2$ for any s, t in this case, we have $r_k - r_h \ge 4$ for $h < k-1$ and $r_h - r_k \ge 3$ for $h > k$ and it follows that $Q(v) \in Q(A_{k-1}X_{k-1} + A_k X_k)\dot{F}^2$. So assume minimality occurs only at the index k. Then $|A_k| \ge |2|$ since $S_v \in O(\tilde{L})$. Suppose $A_k \in \mathfrak{u}_{\mathfrak{p}}$ and that $r_{k+1} - r_k = 1$. We treat here the case $r_{k+1} = r_k + 1$. If $j > k+1$, then $r_j - r_k \ge 4$ and $Q(A_j X_j) \in 8Q(v)\mathfrak{o}$ and similarly if $j < k$ with $r_k - r_j \ge 4$. If $r_k = r_{k-1} + 3$ and $A_{k-1} \in 4\mathfrak{u}_{\mathfrak{p}}$, we have $|Q(A_{k-1}X_{k-1})| = |2|\,|Q(v)|$ and a calculation shows that

$$Q(A_{k-1}X_{k-1} + A_{k+1}X_{k+1}) = A_{k+1}^2 2^{r_k+1}(a_{k-1}\varepsilon^2 + a_{k+1})$$

where $\varepsilon \in \mathfrak{u}_{\mathfrak{p}}$. The last factor, being a sum of units of defect $\subseteq \mathfrak{p}^3$, lies in $2\mathfrak{o}$. That is, $Q(A_{k-1}X_{k-1} + A_{k+1}X_{k+1}) \in 4A(v)\mathfrak{o}$. On the other hand, if $A_{k+1} \in \mathfrak{p}$, then $Q(A_{k+1}X_{k+1}) \in 4Q(v)\mathfrak{o}$ and $Q(v) \in Q(A_{k-1}X_{k-1} + A_k X_k) \times (1 + 4\mathfrak{o})$ and the result follows. Keeping the assumption $r_{k+1} - r_k = 1$, the other possibilities $|A_k| = |\pi|$ and $|A_k| = |2|$ are resolved in a similar manner.

The above argument shows that when there is no index k with $r_{k+1} - r_k = 1$ we have $Q(v) \in \mathfrak{u}_{\mathfrak{p}}\dot{F}^2$ for all $v \in P(\tilde{L})$. If this is the case and there are indices l, t, and s with $r_{l+1} - r_l = 3$ and $r_t - r_s = 2$ the result again follows since $\theta(O^+(\tilde{L})) = \mathfrak{u}_{\mathfrak{p}}\dot{F}^2$. So to complete the proof we need only verify the result for a $v \in P(\tilde{L})$ whose value equals $|Q(A_k X_k)|$ and $r_k - r_{k-1} \ge 3$ and $r_{k+1} - r_k \ge 3$. This can be easily done using an argument analogous to the one given above. QED

When L does not have the diagonal decomposition discussed above,

$\theta(O^+(\tilde{L}))$ contains $\mathfrak{u}_p \dot{F}^2$ since this is the spinor norm group for *any* modular component of dimension greater than one. The exact value is then calculated by the following theorems.

Theorem 2.18 *Let $m \equiv 3 \pmod 4$ and L have a Jordan component of dimension greater than one. Then $\theta(O^+(\tilde{L})) = \mathfrak{u}_p \dot{F}^2$ if and only if L is not split by a sublattice $2^r\langle \varepsilon, 2\gamma\rangle$, $\varepsilon, \gamma \in \mathfrak{u}_2$. If L is split in this way, then $\theta(O^+(\tilde{L})) = \dot{F}$.*

The second statement is clear since $\theta(O^+(\langle \varepsilon, 2\gamma\rangle))$ has index two in $\dot{F}$. The first follows immediately from the following lemma, which is proved by induction on the number of Jordan components in a splitting of L.

Lemma 2.19 *If L is not split by a sublattice of the type $2^r\langle \varepsilon, 2\gamma\rangle$, then $\theta(O^+(\tilde{L})) \subseteq \mathfrak{u}_p \dot{F}^2$.*

3. Applications

In Earnest and Hsia [6] a construction was given that produced a lattice L having arbitrary dimension d and $g^+(L) = 2^n$ for any prescribed integer n. Now, additionally, let k be any positive integer with $k \leq n$. We now give an alternative construction of a lattice L having both the properties above but also for which an infinite number of extensions $E = \mathbb{Q}(\sqrt{m})$ can be constructed so that $|\mathrm{Ker}(\psi_L)| = 2^k$ in each of these extensions.

Example 3.1 Let $q_1, \ldots, q_n$ be distinct odd primes for which the Legendre symbol $(2/q_i) = 1$ for $i = 1, \ldots, n$. The lattice $L = \langle 1, \beta^2, \ldots, \beta^{2(d-1)}\rangle$ has dimension d and $g^+(L) = 2^n$, as can be easily calculated using the technique described in Section 1. In particular, the primes q_i may be chosen so that $q_i \equiv 1 \pmod 8$ for each $i = 1, \ldots, n$.

Proposition 3.2 *There are infinitely many extensions $E = \mathbb{Q}(\sqrt{m})$ for which $|\mathrm{Ker}(\psi_L)| = 2^k$ where the lattice L is constructed as above.*

Proof Let p be a prime that satisfies:

(i) $p \equiv 3 \pmod 8$;
(ii) $(p/q_i) = -1$ for $i = 1, \ldots, k$;
(iii) $(p/q_i) = +1$ for $i = k+1, \ldots, n$.

We claim that when $E = \mathbb{Q}(\sqrt{-p})$, $|\mathrm{Ker}(\psi_L)| = 2^k$. First note that $-p \in \Delta_{q_i} \dot{\mathbb{Q}}_{q_i}^2$ for $i = 1, \ldots, k$. So the idèles $j(i)$ defined by

$$(j(i))_q = \begin{cases} \Delta_q & \text{if } q = q_i \\ 1 & \text{otherwise} \end{cases}$$

all have the property that $\psi_L(\overline{j(i)}) = (\bar{1})$ for $i = 1, \ldots, k$; hence $|\mathrm{Ker}(\psi_L)| \geq 2^k$. It remains only to show that no element $j = \prod_{i=k+1}^{n} j(i)^{\varepsilon_i}$,

$\varepsilon_i \in \{0, 1\}$, becomes trivial in $\mathscr{G}_E(\tilde{L})$. By Theorem 1.7, $\bar{j} \in \mathrm{Ker}(\psi_L)$ if and only if $h(j) \in \gamma J_E^L$ where γ is a product of the elements -1, 2, and p. Since $q_i \equiv 1 \pmod 8$, -1 and 2 are squares in $\hat{\mathbb{Q}}_{q_i}^2$ and the choice of p assures $p \in \hat{\mathbb{Q}}_{q_i}^2$ for $i = k+1, \ldots, n$. Thus, $|\mathrm{Ker}(\psi_L)| = 2^k$.

The p used above can be chosen to be any prime that is a solution of the linear congruence system

$$\begin{aligned} Y &\equiv 3 \pmod 8 \\ Y &\equiv t_1 \pmod{q_i} \\ &\vdots \\ Y &\equiv t_n \pmod{q_n} \end{aligned}$$

where $t_i \in \mathbb{Z}$ satisfy $(t_i/q_i) = -1$, $i = 1, \ldots, k$ and $(t_i/q_i) = +1$ for $i = k+1, \ldots, n$. QED

Remark 3.3 For the lattices L and extensions E constructed above, it can be shown that, although the map ψ_L is not injective, the number $g^+(\tilde{L})$ is at least as large as $g^+(L)$. The next example will show that the value of g^+ may decrease in passing from $\mathbb{Q}$ to E.

Example 3.4 Consider the space $V = [1, 1, -1, -1]$ over $\mathbb{Q}$. Let K be the $\mathbb{Z}$-lattice on V given by $K \cong \langle -1, -5^2, 5^4, 5^6 \rangle$ and let J_2 be the lattice on V_2 given by

$$J_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \perp \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

By 81 : 14 of [12], there is a lattice L on V for which $L_p \cong K_p$ for p odd and $L_2 \cong J_2$. This lattice L has $g^+(L) = 2$ but $g^+(\tilde{L}) = 1$.

By using the machinery established in Earnest and Hsia [6, 7], and Section 2, sufficient conditions in terms of the lattice L and the extension E, for the number g^+ to be nondecreasing in passing from $\mathbb{Q}$ to $E = \mathbb{Q}(\sqrt{m})$, can be obtained. Another group homomorphism η can be constructed, $\eta: \mathscr{G}_{\mathbb{Q}}(L) \to \mathscr{G}_E(\tilde{L})$, and shown to be injective under the given condition. Details of the construction can be found in Earnest [2]. Let $\mathscr{S}(E)$ denote the set of all rational primes that divide $\mathrm{disc}(E/\mathbb{Q})$.

Theorem 3.5 *Let L be a $\mathbb{Z}$-lattice,* $\dim L \geq 3$. *Then*

$$\mathscr{E}'(L) \cap \mathscr{S}(L) = \varnothing \Rightarrow g^+(\tilde{L}) \geq g^+(L).$$

Corollary 3.6 *If no rational prime divides both* $\mathrm{disc}(E/\mathbb{Q})$ *and* $\det L$, *then* $g^+(\tilde{L}) \geq g^+(L)$.

The computations in Section 2 can be used to generalize to quadratic exten-

sions the results of Kneser [11] and Earnest and Hsia [5] giving sufficient conditions, in terms of the reduced determinant of a $\mathbb{Z}$-lattice L, for the number $g^+(L)$ to be one. We obtain here a somewhat weaker condition which guarantees only that $g^+(\tilde{L}) = 1$ when L is lifted into a quadratic extension with odd ideal class number.

Notation used here will conform to that introduced in Earnest and Hsia [5]. In particular, define $d'L$ to be $d'L = \det(L^{a^{-1}})$ where $nL = a\mathbb{Z}$. If $\delta(L)$ denotes reduced determinant defined in Eichler [8], $d'L$ is related to $\delta(L)$ by the formula $\delta(L) = 2^n(d'L)\mathbb{Z}$. Note in particular that, in contrast to $\delta(L)$, $d'L$ is not always an integer but may be rational with 2-power denominator. So $d'L = \prod_p p^{s_p}$ with $s_p \in \mathbb{Z}$ and s_p positive for p odd (s_2 may be negative).

Let $E = \mathbb{Q}(\sqrt{m})$ and let the ideal class number of E be $h_E = h_2(E) \cdot h_0(E)$ where $h_2(E)$ is a power of 2 and $h_0(E)$ is odd. We seek to determine the *best possible* bound $\mathscr{B}$ so that the conditions

(i) $s_p < (n(n-1))/2$, $n = \dim L$,
(ii) $s_2 < \mathscr{B}$

will imply that $g^+(\tilde{L}) \leq h_2(E)$ (or that $g^+(\tilde{L}) \leq 2h_2(E)$ when L definite, $m > 0$ with $N_{E/\mathbb{Q}}(\varepsilon) = -1$). In particular, when h_E is odd, we obtain $g^+(\tilde{L}) = 1$ (or $g^+(\tilde{L}) \leq 2$, respectively). The bound $\mathscr{B}$ varies depending upon the field E. Of course, if 2 is unramified in E, then the bound $\mathscr{B}$ is exactly as determined in [5]. So we restrict our interest to the cases $m \equiv 2, 3 \pmod 4$. The proofs of the following results are consquences of the results of Section 2 and the index computations in Earnest [3].

Proposition 3.7 (i) *If $m \equiv 2 \pmod 4$, the best possible value of $\mathscr{B}$ is*

$$B = \frac{n(n-3)}{2} + \left[\!\left[\frac{n+1}{2}\right]\!\right]$$

when $m < 0$ or $m > 0$ with $N_{E/\mathbb{Q}}(\varepsilon) = +1$ (ε denotes the fundamental unit of E).

(ii) *If $m \equiv 2 \pmod 4$, $m > 0$ with $N_{E/\mathbb{Q}}(\varepsilon) = -1$ and the lattice L is indefinite, then the best possible bound $\mathscr{B}$ is $2n(n-1)$.*

[Examples showing the given bounds are best possible are $L = \perp_{i=0}^{(n-2)/2} \langle 2^{2i} \rangle A(1, 2)$ in case (i) and $L = \langle -7 \rangle \perp (\perp_{i=1}^{n-1} \langle 2^{4i} \rangle)$ in case (ii).]

Remark 3.8 In case $m \equiv 3 \pmod 4$, it is not as easy to determine the best possible value of $\mathscr{B}$. If $m < 0$, the result is as follows:

(i) For $m = -1$, best possible value is $B'' = n(n-1)$.
(ii) For $m \neq -1$, best possible value is $B' = n(n-1) - [\![n/2]\!]$.

For $m > 0$, the best possible bound may be either B', B'', $\frac{3}{2}B''$, or $2B''$ and the

precise value can be determined by checking whether $\pm 2 \in N_{E/\mathbb{Q}}(\dot{E})$, whether the trace $\mathrm{Tr}_{E/\mathbb{Q}}(\varepsilon) \equiv 0 \pmod 4$ and by evaluating the symbol $(\varepsilon, f)_{\mathfrak{p}}$ where $\mathfrak{p} \mid 2$ and $2 = \pi^2 f$ in $E_{\mathfrak{p}}$.

Remark 3.9 Precise values of $g^+(\tilde{L})$ are determined for *unimodular* lattices L in [3]. Also obtained as a consequence of the index computations there is a crude upper bound for the values of $g^+(\tilde{L})$ for an arbitrary L.

REFERENCES

[1] N. C. Ankeny and J. S. Hsia, Unimodular round forms over dyadic local fields, *J. Number Theory* **6** (1974), 443–447.
[2] A. G. Earnest, Spinor norms and spinor genera of integral quadratic forms under field extensions, Ph.D. Dissertation, Ohio State Univ., Columbus, Ohio, 1975.
[3] A. G. Earnest, Spinor genera of unimodular $\mathbb{Z}$-lattices in quadratic fields, *Proc. Amer. Math. Soc.*, to appear.
[4] A. G. Earnest and J. S. Hsia, Springer-type theorems for spinor genera of quadratic forms, *Bull. Amer. Math. Soc.* **81** (1975), 942–943.
[5] A. G. Earnest and J. S. Hsia, Spinor norms of local integral rotations, II, *Pacific J. Math.* **61** (1975).
[6] A. G. Earnest and J. S. Hsia, Spinor genera under field extensions, I, *Acta Arith.*, to appear.
[7] A. G. Earnest and J. S. Hsia, Spinor genera under field extensions, II: 2 unramified in the bottom field, *Amer. J. Math.*, to appear.
[8] M. Eichler, "Quadratische Formen und orthogonale Gruppen." Springer-Verlag, Berlin–Göttingen–Heidelberg, 1952.
[9] J. S. Hsia, Spinor norms of local integral rotations, I, *Pacific J. Math.* **57** (1975), 199–206.
[10] G. Janusz, "Algebraic Number Fields." Academic Press, New York, 1973.
[11] M. Kneser, Klassenzahlen indefiniter quadratischer Formen in drei oder mehr Veränderlichen, *Arch. Math. (Basel)* **7** (1956), 323–332.
[12] O. T. O'Meara, "Introduction to Quadratic Forms." Springer-Verlag, Berlin–Göttingen–Heidelberg, 1963.
[13] O. T. O'Meara and B. Pollak, Generation of local integral orthogonal groups, I, *Math. Ze.* **87** (1965), 385–400.
[14] O. T. O'Meara and B. Pollak, Generation of local integral orthogonal groups, II, *Math. Ze.* **93** (1966), 171–188.

AMS (MOS) 1970 subject classifications: 10C05, 15A63.

On Products of Consecutive Integers

P. ERDÖS

HUNGARIAN ACADEMY OF SCIENCE
BUDAPEST, HUNGARY

E. G. STRAUS†

UNIVERSITY OF CALIFORNIA
LOS ANGELES, CALIFORNIA

1. Introduction

We define $A(n, k) = (n + k)!/n!$ where n, k are positive integers and we wish to examine divisibility properties of $A(n, k)$.

First observe that the cases $k = 1, 2$ are special. The relations

$$tA(n, 1) = A(m, 1) \qquad \text{and} \qquad tA(n, 2) = A(m, 2)$$

each have infinitely many solutions n, m—the first for every positive integer t; the second for every positive integer that is not a square, as can be seen from Pell's equation

$$(2m + 1)^2 - t(2n + 1)^2 = 1 - t.$$

On the other hand, it is well known from the Thue–Siegel theorem that for given $k \geq 3$ and fixed $t > 1$ the equation

$$tA(n, k) = A(m, k) \tag{1.1}$$

has only a finite number of solutions in integers n, m.

† Research of the second author was supported in part by Grant MCS 76-06988.

It is possible that (1.1) has only a finite number of solutions for fixed t and variable $k > 2$, but we cannot prove this even in the case $t = 2$ without additional hypotheses on n. Perhaps the following stronger conjecture holds: $A(n, k) = tA(m, l)$ has only a finite number of solutions $m \geq n + k$ for every rational t if $\min(k, l) > 1$, $\max(k, l) > 2$.

Let $f(n, k)$ be the least positive integer $m > n$ so that

$$A(m, k) \equiv 0 \pmod{A(n, k)}. \tag{1.2}$$

We obviously have $f(n, k) \leq A(n, k) - k$ and it is easy to see that for $k > 1$ we get several residue classes (in addition to $-k$) (mod $A(n, k)$) for m which ensure that (1.2) holds. The number of these residue classes is always larger than k, in fact exponential in k, so that the above inequality on $f(n, k)$ can always be improved.

The algebraic identities

$$x(x+1)(x+2) = (x^2 + 2x)(x+1)$$

$$\text{which divides } (x^2 + 2x)(x^2 + 2x + 1)$$

$$x(x+1)(x+2)(x+3) = (x^2 + 3x)(x^2 + 3x + 2)$$

$$x(x+1)(x+2)(x+3)(x+4) = (x^2 + 4x)(x^2 + 4x + 3)(x+2)$$

$$\text{which divides } (x^2 + 4x)(x^2 + 4x + 3)(x^2 + 4x + 4)$$

show that $A(n, 3)$ divides $A(n^2 + 4n + 1, 3)$; $A(n, 4)$ divides $A(n^2 + 5n + 2, 4)$; and $A(n, 5)$ divides $A(n^2 + 6n + 4, 5)$. Thus $f(n, 3) \leq n^2 + 4n + 1$, $f(n, 4) \leq n^2 + 5n + 2$, $f(n, 5) \leq n^2 + 6n + 4$. It seems likely that these bounds are attained for infinitely many, perhaps for almost all, values of n. One might ask whether we get $f(n, k) < n^{k-\delta}$ for all (almost all) large n and some $\delta > 0$ when $k > 5$. In the other direction we would like to know whether $f(n, k) > n^{1+\delta}$ for infinitely many (almost all) n for some $\delta > 0$ when $k > 1$. For $k = 2$, we have infinitely many n with $f(n, k) \sim \sqrt{2n}$. Are there infinitely many n with $f(n, k) < cn$ for fixed c, $k > 2$?

A function closely related to $f(n, k)$ is $g(n, k)$, the minimal integral value $A(m, k)/A(n, k)$, $m > n$. The above discussion shows that $g(n, k) \sim f(n, k)^k/A(n, k)$ for fixed k and thus $g(n, k) \ll n^k$ for $k \leq 5$. Table 1 gives values of $f(n, k)$, $g(n, k)$ for small n and k.

One may try to estimate the density $d(n, k)$ of integers m for which (1.2) holds. Obviously $d(n, 1) = 1/(n + 1)$. For $k = 2$ we have

$$d(n, 2) = 2^{\omega(A(n, 2))}/A(n, 2), \tag{1.3}$$

where $\omega(x)$ denotes the number of distinct prime factors of x. Relation (1.3) follows from the fact that $A(m, 2)$ is divisible by $A(n, 2)$ if and only if we can

TABLE 1

n \ k	1		2		3		4		5		6		7	
	f	g	f	g	f	g	f	g	f	g	f	g	f	g
1	3	2	2	2	3	5	2	3	4	21	2	4	3	15
2	5	2	7	6	3	2	6	14	4	6	3	3	5	22
3	7	2	14	12	7	6	4	2	11	78	6	11	13	646
4	9	2	8	3	12	13	6	3	13	68	22	1794	20	2691
5	11	2	13	5	13	10	52	2915	13	34	6	2	17	437
6	13	2	47	42	25	39	52	1749	17	57	16	969	7	2
7	15	2	62	56	53	231	52	1113	31	476	50	18921	21	345
8	17	2	34	14	42	86	32	119	50	2703	50	10812	20	138
9	19	2	43	18	19	7	51	477	51	1908	20	46	59	68076
10	21	2	31	8	63	160	62	720	51	1272	60	11346	49	11925
11	23	2	38	10	25	9	24	15	60	1891	46	1645	62	33902
12	25	2	76	33	62	96	61	372	47	420	50	1749	50	5247
13	27	2	19	2	47	35	31	22	31	42009	151	695981	169	11865205
14	29	2	79	27	117	413	268	72899	131	30954	284	20233213	149	3346915
15	31	2	254	240	269	4065	302	92415	319	1860516	284	14452295	169	5393275

factor $A(n, 2)$ into two relatively prime divisors $A(n, 2) = d_1 d_2, (d_1, d_2) = 1$, and require

$$m \equiv -1 \pmod{d_1}, \qquad m \equiv -2 \pmod{d_2}.$$

Since there are $2^{\omega(A(n, 2))}$ such factorizations of $A(n, 2)$, we get that many residue classes (mod $A(n, 2)$) for m.

For $k > 2$, the problem of computing $d(n, k)$ becomes messier, but not intrinsically difficult. The number of residue classes (mod $A(n, k)$) to which m must belong remains $O(n^{\varepsilon})$ for every $\varepsilon > 0$ and hence

$$\frac{1}{n^k} \ll d(n, k) \ll \frac{1}{n^{k-\varepsilon}}$$

for all values of k.

Another question is that of determining those $m > n$ so that there exists some k for which (1.2) holds. Since for $k > m - n$, we have

$$\frac{A(m, k)}{A(n, k)} = \frac{A(n + k, m - n)}{A(n, m - n)},$$

which is certainly an integer for $k = A(n, m - n) - m$, the problem becomes trivial unless we restrict the values of k to $k \leq m - n$.

For $n = 1$ and any m we see that

$$\frac{A(m, p - 1)}{A(1, p - 1)} = \frac{1}{p}\binom{m + p - 1}{p - 1}$$

is divisible by p unless $m \equiv 0 \pmod{p}$. Since m cannot be divisible by all primes $\leq m$ except when $m = 2$, we see that for every $m > 2$ there exists a k, $1 \leq k \leq m-1$ so that $A(1, k)$ divides $A(m, k)$. The question whether there exists a k, $1 \leq k \leq m-2$, so that $A(2, k)$ divides $A(m, k)$, which is equivalent to $\binom{k+2}{2}$ divides $\binom{m+k}{k}$, seems much more difficult to decide. The general problem can be stated as follows:

Given $n > 1$ is it true that for all (almost all) large m there exists a k, $1 \leq k \leq m-n$ so that

$$\binom{k+n}{n} \Big| \binom{m+k}{k} ? \tag{1.4}$$

If not, what is the density $d^*(n)$ of integers m for which (1.4) has a solution with $1 \leq k \leq m-n$?

In Section 2 we show that for bounded ratios m/n and any $\delta > 0$ we get only a finite number of solutions of (1.2) with $k > \delta n$.

In Section 3 we treat the special case in which the set $\{n+1, \ldots, n+k\}$ contains a prime and m/n is bounded to show that (1.2) has only a finite number of solutions $2 \leq k \leq m-n$ in that case. We give an example which may prove the only one with $m \leq 2n$. Finally, we mention some additional problems and conjectures.

2. The Case $k \geq \delta n$

In this section we prove the following.

Theorem 2.1 *Given positive numbers δ, Δ so that $k \geq \delta n$ and $n + k \leq m \leq \Delta n$, then there exists an $n_0 = n_0(\delta, \Delta)$ so that the congruence* (1.2) *has no solution with $n \geq n_0$.*

The proof depends on showing that for all large n there exists a prime p in the interval $[n+1, n+k]$ that divides $A(n, k)$ to a higher power than it divides $A(m, k)$.

Lemma 2.2 *Assume that the hypotheses of Theorem* 2.1 *are satisfied and that every prime $p \in [n+1, n+k]$ divides $A(m, k)$. Then for every $\varepsilon > 0$ there exists an $n_1 = n_1(\varepsilon)$ so that for all $n \geq n_1$ there exists an integer l, $2 \leq l < \Delta$, with*

$$(l - \varepsilon)n + (l-1)k < m < lk + \varepsilon n \tag{2.1}$$

and hence

$$(l - 2\varepsilon)n < k. \tag{2.2}$$

Note that it is possible to have every prime that divides $A(n, k)$ also divide $A(m, k)$. This always happens when $k = ln$, $m = l^2 n$.

Proof Let n be so large that there exists a prime in $[n+1, n+k]$ and let p be the largest prime in that interval. Let l be the largest integer so that $lp \le m+k$. Then $l \ge 2$ and for large n we have $p > n+k-\delta n$. Hence

$$l \le \frac{m+k}{p} < \frac{m+k}{n+k-\delta n} < 1 + \frac{m-n}{(1+\delta-\delta)n} < 1 + \Delta - 1 = \Delta.$$

Now pick n so large that $p > n+k-\varepsilon n/\Delta$. Then

$$m+k \ge lp > ln + lk - \varepsilon n$$

and hence

$$(l-\varepsilon)n + (l-1)k < m.$$

Let q be the smallest prime so that $m+k < (l+1)q$. For large n we must have $n < q$ since otherwise l times every prime in $[n+1, n+k]$ would lie in $[m+1, m+k]$, which is impossible. Let n be so large that

$$\frac{m+k}{l+1} < q < \frac{m+k}{l+1} + \frac{\varepsilon n}{l(l+1)},$$

then $m < lq$ and hence

$$(l+1)m < l(m+k) + \varepsilon n$$

or

$$m < lk + \varepsilon n.$$

Lemma 2.3 *Assume that the hypotheses of Theorem* 2.1 *are satisfied and that* s *is an integer such that* $n < k/s$ *and every prime* $p \in [k/t, (n+k)/t]$, $t = 1, 2, \ldots, s$, *satisfies*

$$A(m, k) \equiv 0 \pmod{p^t}.$$

Assume further that for the integer l *in Lemma* 2.2 *we have*

$$m + \frac{a}{b}k - \varepsilon n < l(n+k) < m + \frac{c}{d}k + \varepsilon n \tag{2.3}$$

where a/b *and* c/d *are consecutive terms in the Farey series of order* s *and* ε *is a given number,* $0 < \varepsilon < s^{-2}$.

Then there exists an $n_2 = n_2(\varepsilon)$ *so that for all* $n \ge n_2$ *we have*

$$(l-\varepsilon)n + \left(l - \frac{c}{d}\right)k < m < \left(l - \frac{a}{b}\right)k + \varepsilon n \tag{2.4}$$

and hence

$$k > bd(l-2\varepsilon)n \ge s(l-2\varepsilon)n. \tag{2.5}$$

Proof For $s = 1$, this is Lemma 2.2. We now proceed by induction on s. If $\max\{b, d\} < s$, then the result follows from the induction hypothesis.

If $d = s > 1$, then $b < s$ and the first inequality in (2.4) follows directly from (2.3) while the second inequality holds by the induction hypothesis.

Now assume that $b = s$, $d < s$. Then the first inequality in (2.4) is still an immediate consequence of (2.3). If the second inequality were false, we would have

$$sl\frac{k}{s} < m + \frac{a}{s}k - \varepsilon n < sl\frac{n+k}{s}.$$

If $l(n+k) \leq m + (a/s)k + \varepsilon n$ and n is sufficiently large, then there exists a prime p so that

$$m + \frac{a}{s}k - 2\varepsilon n < slp < m + \frac{a}{s}k + \varepsilon n \qquad \text{and} \qquad \frac{n+k}{s} - \frac{\varepsilon n}{sl} < p < \frac{n+k}{s}.$$

Hence $(sl - a)p \leq m$ and $(sl + s - a)p > m + k$ and $A(m, k) \not\equiv 0 \pmod{p^s}$, contrary to hypothesis.

We may therefore assume that $l(n+k) > m + (a/s)k + \varepsilon n$; then for large n there exists a prime p with

$$m + \frac{a}{s}k < slp < m + \frac{a}{s}k + \frac{\varepsilon n}{sl} \qquad \text{and} \qquad \frac{k}{s} + \frac{\varepsilon n}{sl} < p < \frac{n+k}{s}.$$

Thus, again, $(sl - a)p \leq m$ while $(sl + s - a)p > m + k$ and $A(m, k) \not\equiv 0 \pmod{p^s}$, contrary to hypothesis.

Proof of Theorem 2.1 If $l > 2$ and every prime $p \in [k/2, (n+k)/2]$ satisfies $A(m, k) \equiv 0 \pmod{p^2}$, then, according to (2.5), we have $k > 3n$. Now let s be the largest integer for which $sn < k$. If every prime $p \in [k/t, (n+k)/t]$, $t = 1, 2, \ldots, s$ satisfies $A(m, k) \equiv 0 \pmod{p^t}$, then, according to (2.5), we have $k > s(2 - 2\varepsilon)n > (s+1)n$, a contradiction.

Now if $l = 2$ and $2n < k$, then Lemma 2.3 can be applied as before. If $l = 2$ and $2n \geq k$, then every prime $p \in [n+1, (n+k)/2]$ satisfies $A(n, k) \equiv 0 \pmod{p^2}$. But, according to Lemma 2.2, we have

$$(4 - 3\varepsilon)n < m < m + k < (6 + \varepsilon)n.$$

Thus for large n there exists a prime p,

$$(\tfrac{5}{4} - \varepsilon)n < p < (\tfrac{5}{4} + \varepsilon)n,$$

so that for sufficiently small ε we have $3p < m$ while $5p > m + k$ and $A(m, k) \not\equiv 0 \pmod{p^2}$.

3. The Case $A(m, k) \equiv 0 \pmod{A(n, k)}$; $n + k \leq m \leq \Delta n$ and $\{n + 1, \ldots, n + k\}$ Contains a Prime

We first mention the interesting example

$$A(32, 6) = 37 \cdot A(16, 6). \tag{3.1}$$

Here two of the integers 17, 18, 19, 20, 21, 22 are primes and 17 may well be the largest n which solves our problem in case $\Delta = 2$. In the following we show that we can find an effective bound for all solutions k, n, m.

From Theorem 2.1 we know that we can restrict attention to cases $k < \delta n$ where δ is any fixed positive number. Since there exists a prime p with

$$n + 1 \leq p \leq n + k \leq m \leq \Delta n \tag{3.2}$$

and $A(m, k)/A(n, k)$ is an integer, there must exist an integer l so that

$$m + 1 \leq lp \leq m + k. \tag{3.3}$$

Thus

$$ln + l - k \leq m \leq ln + (l - 1)k. \tag{3.4}$$

Lemma 3.1 *Every integer*

$$x \in [n + 1, n + k]\left[\frac{m + 1}{l}, \frac{m + k}{l}\right]$$

has all prime divisors less than $(l + 1)k$.

Proof Assume that x has a prime divisor $q > (l + 1)k$. Now, either $lx < m + 1$ and $lx + q > ln + lk \geq m + k$ so that q does not divide $A(m, k)$, or $lx > m + k$ and $lx - q < ln + lk - (l + 1)k < m$ and again q does not divide $A(m, k)$.

The set of integers in $[n + 1, n + k]\backslash[(m + 1)/l, (m + k)/l]$ contains an interval of length $\geq k(l - 1)/2l = ks$.

Lemma 3.2 *There exists a* k_0 *so that* $A(n, [ks])$ *has prime divisors greater than* $(l + 1)k$ *for all* $k \geq k_0$, $k \leq \delta n$.

Proof Set $[ks] = t$ and consider the binomial coefficient

$$\binom{n + t}{t} = \frac{A(n, t)}{t!}$$

Every prime power q^α that divides a binormal coefficient $\binom{n+t}{t}$ satisfies $q^\alpha \leq n + t$. Thus the hypothesis that all prime divisors are $< (l + 1)k$ yields

$$\binom{n + t}{t} \leq (n + t)^{\pi((l+1)k)} < (n + t)^{c(l+1)k/\log k} \tag{3.5}$$

for a suitable constant c. On the other hand

$$\binom{n+t}{t} \geq \left(\frac{n+t}{t}\right)^t. \tag{3.6}$$

Now set $(n+t)/t = C > 1/\delta$ and compare (3.5) and (3.6) to get

$$C^t < C^{c(l+1)k/\log k}(sk)^{c(l+1)k/\log k} \tag{3.7}$$

which is false for $k > k_0$ provided δ is small enough.

Theorem 3.3 *For each $\Delta > 1$ there exists only a finite number of integers k, n, m such that $k > 1, n + k \leq m \leq \Delta n$ and $A(m, k) \equiv 0 \pmod{A(n, k)}$ where the interval $[n+1, n+k]$ contains a prime.*

Proof We first pick δ in Theorem 2.1 sufficiently small and then can restrict attention to a fixed integer l, $2 \leq l \leq \Delta + \delta$. By Lemma 3.2 we have $k < k_0$. Now pick one of the integers $x \in [n+1, n+k]$ so that $lx \notin [m+1, m+k]$. Then, by the same argument that we used in the proof of Lemma 3.1 we have $(x, y) < (l+1)k$ for every $y \in [m+1, m+k]$ and hence, if $x \mid A(m, k)$ we must have $n < x < ((l+1)k)^k < ((l+1)k_0)^{k_0}$.

We have not carried out the detailed estimates needed to show, for example, that the example stated at the beginning of this section is the unique solution for $\Delta = 2$, except for $A(4, 2)$ and $A(8, 2)$, but it would not be difficult to do so.

4. Open Questions

4.1. In view of Lemma 2.2, it would be interesting to know the smallest $m > 2k$ so that every prime in the interval $[k+1, 2k]$ divides $A(m, k)$. In particular, is it true that $m \gg k^c$ for every c?

4.2. We know of no example with $n > 16$, $k > 2$, where $A(n, k)$ divides $A(m, k)$ and $n + k \leq m \leq 2n$. It would be interesting to find a bound for such n without the hypothesis that there exists a prime in the interval $[n+1, n+k]$.

4.3. A question related to those discussed in this paper is to find solutions for $A(n, k) \mid A(n+k, n+2k)$. Charles Grinstead has found the following examples:

n:	2	3	4	5	6	7	8	9
k:	4	3	206	1886	3472	3471	8170	8169

AMS (MOS) 1970 subject classification: 10A05.

Non-Abelian Jacobi Sums

A. FRÖHLICH

KING'S COLLEGE
UNIVERSITY OF LONDON
LONDON, ENGLAND

Introduction

The Gauss sums for multiplicative characters of finite fields, which play such an important role in classical number theory, appear again in the functional equation of Abelian L-functions, as local Gauss sums $\tau_{\mathfrak{p}}(\chi)$ for prime ideals $\mathfrak{p}$ which are tame at χ, i.e., divide the conductor to at most the first power. Going over to Artin L-functions, one gets analogously tame local Galois Gauss sums for arbitrary characters of Galois groups, derived from the local constants of Langland. For details see, e.g., Martinet [4].

For tame Abelian local Gauss sums, the quotient

$$j_{\mathfrak{p}}(\chi, \phi) = \tau_{\mathfrak{p}}(\chi)\tau_{\mathfrak{p}}(\phi)\tau_{\mathfrak{p}}(\phi\chi)^{-1},$$

in the nontrivial case when $\mathfrak{p}$ is actually ramified at χ, ϕ, and $\chi\phi$, is a Jacobi sum, hence an algebraic integer. We shall be concerned with the corresponding "non-Abelian Jacobi sum"

$$j_{\mathfrak{p}}(\chi, \phi) = \tau_{\mathfrak{p}}(\chi)^{\deg(\phi)}\tau_{\mathfrak{p}}(\phi)^{\deg(\chi)}\tau_{\mathfrak{p}}(\chi\phi)^{-1}, \tag{0.1}$$

$\deg(\chi)$ denoting the degree of χ, always under the hypothesis that $\mathfrak{p}$ be tame

at χ and ϕ. From the connection between Galois Gauss sums and Galois module structure of algebraic integers (cf. Fröhlich [1]) and using the theory of module resolvents (cf. Fröhlich [2]), we shall derive an interpretation of the fractional ideals generated by the $j_{\mathfrak{p}}(\chi, \phi)$ which then implies that they are integral. This interpretation is new and of interest even in the classical absolutely Abelian case. Our method will also yield, without further effort, a similar interpretation for the quotients of local conductors, which, however, lies less deep.

1. Statement of Results

Let $\bar{Q}$ be the algebraic closure of Q in the field of complex numbers. A number field K is always a subfield of $\bar{Q}$ of finite degree over Q, and we write $\mathrm{Gal}(\bar{Q}/K) = \Omega_K$. Throughout N/K is a normal extension of number fields with Galois group Γ and $\mathfrak{p}$ is a finite prime divisor of K which, except for Theorem 1, will be assumed to be tame (i.e., at most tamely ramified) in N. If χ, ϕ are characters of Γ, then $j_{\mathfrak{p}}(\chi, \phi)$ is defined as in (0.1), and $k(\chi, \phi)$ is the field obtained by adjoining to the number field k the values of χ and ϕ on Γ.

Theorem 1 *For* $\omega \in \Omega_Q$,

$$j_{\mathfrak{p}}(\chi^{\omega}, \phi^{\omega}) = j_{\mathfrak{p}}(\chi, \phi)^{\omega}.$$

In particular $j_{\mathfrak{p}}(\chi, \phi) \in Q(\chi, \phi)$.

This theorem can be proved quickly. Observe that $j_{\mathfrak{p}}(\chi, \omega)$ is the local Galois Gauss sum $\tau_{\mathfrak{p}}(\theta)$ for the virtual character $\theta = \deg(\phi)\chi + \deg(\chi)\phi - \chi\phi$, and that $\det_\theta = 1$ on Γ. Then apply the formula for Galois action in Martinet [4, II, Theorem 5.1].

Denote by $R(\Gamma)$ the group ring of Γ over a ring R. Let E be a number field containing K, and let V, W be $E(\Gamma)$-modules of finite dimension. Γ will also act on the algebra $N \otimes_K E$ via the first factor. If $f\colon V \to N \otimes_K E$, $g\colon W \to N \otimes_K E$ are homomorphisms of $E(\Gamma)$-modules so is the product fg given by

$$V \otimes_E W \xrightarrow{f \otimes g} (N \otimes_K E) \otimes_E (N \otimes_K E) \xrightarrow{\text{multiplication}} N \otimes_K E.$$

We get a homomorphism

$$\mu\colon H_V \otimes_E H_W \to H_{V \otimes W} \tag{1.1}$$

with $\mu(f \otimes g) = fg$, where we abbreviate

$$H_V = \mathrm{Hom}_{E(\Gamma)}(V, N \otimes_K E).$$

Theorem 2 *μ is an isomorphism.*

Denote completion at $\mathfrak{p}$ by subscript. Let $\mathfrak{o}$, $\mathfrak{O}$, $\bar{\mathfrak{o}}$ be the rings of algebraic integers of K, N, and E, respectively. Let M, N be lattices over $\bar{\mathfrak{o}}_{\mathfrak{p}}(\Gamma)$, spanning $V_{\mathfrak{p}}$ and $W_{\mathfrak{p}}$, respectively. Abbreviate again

$$H_M = \mathrm{Hom}_{\bar{\mathfrak{o}}_{\mathfrak{p}}(\Gamma)}(M, (\mathfrak{O} \otimes_{\mathfrak{o}} \bar{\mathfrak{o}})_{\mathfrak{p}}).$$

Thus H_M spans $\mathrm{Hom}_{E_{\mathfrak{p}}(\Gamma)}(V_{\mathfrak{p}}, (N \otimes_K E)_{\mathfrak{p}})$ which we identify with $H_{V,\mathfrak{p}}$. We again get a homomorphism

$$\lambda_{\mathfrak{p}}: H_M \otimes H_N \to H_{M \otimes N} \qquad (\otimes = \otimes_{\bar{\mathfrak{o}}_{\mathfrak{p}}}), \tag{1.2}$$

with $\lambda_{\mathfrak{p}}(f \otimes g) = fg$. By Theorem 2 this is injective and has finite cokernel. Moreover cok $\lambda_{\mathfrak{p}}$ is an $\bar{\mathfrak{o}}_{\mathfrak{p}}$-module, hence an $\bar{\mathfrak{o}}$-module. Denote its order over $\bar{\mathfrak{o}}$ by $\mathfrak{T}(M, N)$. This is an ideal of $\bar{\mathfrak{o}}$, where we now take $E = K(\chi, \phi)$, with χ and ϕ the characters of the representations of Γ afforded by V and by W, respectively. Write moreover $\mathfrak{t}(M, N)$ for the order of cok $\lambda_{\mathfrak{p}}$, viewed as a module over the ring $Z(\chi, \phi)$ of algebraic integers in $Q(\chi, \phi)$. Then

$$\mathfrak{t}(M, N) = N_{K(\chi,\phi)/Q(\chi,\phi)}\mathfrak{T}(M, N), \tag{1.3}$$

(norm). Also if $\omega \in \Omega_K$ and M^{ω} is the module obtained from M by semilinear action of ω then

$$\mathfrak{t}(M^{\omega^{-1}}, N^{\omega^{-1}})^{\omega} = \mathfrak{t}(M, N). \tag{1.4}$$

Let now $k = K \cap Q(\chi, \phi)$ and let $\{\sigma\}$ be a right transversal of Ω_k in Ω_Q.

Theorem 3

$$(j_{\mathfrak{p}}(\chi, \phi)) = \prod_{\sigma} \mathfrak{t}(M^{\sigma^{-1}}, N^{\sigma^{-1}})^{\sigma}.$$

Corollary *$j_{\mathfrak{p}}(\chi, \phi)$ is an algebraic integer.*

Next let M^* denote the contragredient $\bar{\mathfrak{o}}_{\mathfrak{p}}(\Gamma)$-module to M, i.e., $M^* = \mathrm{Hom}_{\bar{\mathfrak{o}}_{\mathfrak{p}}}(M, \bar{\mathfrak{o}}_{\mathfrak{p}})$. Let $\mathfrak{f}_{\mathfrak{p}}(\chi)$ be the local conductor.

Theorem 4

$$\mathfrak{f}_{\mathfrak{p}}(\chi)^{\deg(\phi)}\mathfrak{f}_{\mathfrak{p}}(\phi)^{\deg(\chi)}\mathfrak{f}_{\mathfrak{p}}(\chi\phi)^{-1} = \mathfrak{T}(M, N)\mathfrak{T}(M^*, N^*).$$

The corresponding corollary is known, even in the wild case (cf. Martinet [4, Exercise 2]).

2. The Evaluation Pairing

The notation is always that introduced in Section 1. We shall write

$$\pi_V: H_V \otimes_E V \to N \otimes_K E, \qquad \pi_V(f, v) = f(v)$$

for the evaluation pairing. Let $\{f_i\}$, $\{v_i\}$, $\{g_k\}$, $\{w_k\}$ be E-bases of H_V, V, H_W,

and W, respectively. We know that the E-dimensions of H_V and of V coincide and that $\det(f_i(v_j))$ is an invertible element of $N \otimes_K E$. Also

$$\det((f_i g_k)(v_j \otimes w_l)) = (\det(f_i(v_j)))^{\deg(\phi)}(\det(g_k(w_l)))^{\deg(\chi)}, \tag{2.1}$$

where the row index on the left is (i, k), the column index is (j, l). Thus the determinant in (2.1) is invertible and this implies that μ is injective. Counting dimensions we conclude that μ is bijective. This yields Theorem 2.

The above applies equally if we complete at p. Let now $\{f_i\}, \{v_i\}, \{g_k\}, \{w_k\}$ be $\bar{\mathfrak{o}}_\mathfrak{p}$-bases of H_M, M, H_N, and N, respectively. Define

$$\mathfrak{s}(M) = \mathfrak{s}^*(M, (\mathfrak{O} \otimes_\mathfrak{o} \bar{\mathfrak{o}})_\mathfrak{p}) = \bar{\mathfrak{o}}_\mathfrak{p} \det(f_i(v_j)) \tag{2.2}$$

as in Fröhlich [2, §3]. This indeed only depends on M, not on the choice of bases. By (2.1)

$$\mathfrak{s}(M)^{\deg(\phi)}\mathfrak{s}(N)^{\deg(\chi)} = \bar{\mathfrak{o}}_\mathfrak{p} \deg((f_i g_k)(v_j \otimes w_l)). \tag{2.3}$$

The multiplication of the $\bar{\mathfrak{o}}_\mathfrak{p}$-modules on the left of (2.3) is induced by that in $N \otimes_K E$, see, e.g., Fröhlich [2, A.2]. On the other hand, let $\{h_r\}$ be an $\bar{\mathfrak{o}}_\mathfrak{p}$-basis of $H_{M \otimes N}$ ($\otimes = \otimes_{\bar{\mathfrak{o}}_\mathfrak{p}}$). Then via (2.3) we get

$$\mathfrak{s}(M)^{\deg(\phi)}\mathfrak{s}(N)^{\deg(\chi)} = \mathfrak{s}(M \otimes N)\mathfrak{T}(M, N)_\mathfrak{p}, \tag{2.4}$$

following the procedure to compute module indices in this situation given in Fröhlich [2, A.1]. Indeed one can see this easily. If $(a_{(i,k),r})$ is the matrix transforming the basis $\{h_r\}$ of $H_{V \otimes W}$ into the basis $f_i g_k$, then on the one hand

$$\mathfrak{T}(M, N)_\mathfrak{p} = \bar{\mathfrak{o}}_\mathfrak{p} \det(a_{(i,k),r}),$$

while on the other hand

$$\det((f_i g_k)(v_j \otimes w_l)) = \det(a_{(i,k),r}) \det(h_r(v_j \otimes w_l)).$$

Now use (2.1).

Let g be the multiplication $N \otimes_K E \to NE \subset \bar{Q}$, NE the composite field. Apply $g_\mathfrak{p}$ to (2.4) and observe that g acts as the identity on fractional ideals of $\bar{\mathfrak{o}}_\mathfrak{p}$. We get

$$g_\mathfrak{p}(\mathfrak{s}(M))^{\deg(\phi)}g_\mathfrak{p}(\mathfrak{s}(N))^{\deg(\chi)} = g_\mathfrak{p}(\mathfrak{s}(M \otimes N))\mathfrak{T}(M, N)_\mathfrak{p}. \tag{2.5}$$

3. Resolvents

Let $a\mathfrak{o}_\mathfrak{p}(\Gamma) = \mathfrak{O}_\mathfrak{p}$. Let T be a representation of Γ over $\bar{Q}$, corresponding to the character χ. In $\bar{Q}_\mathfrak{p} = \bar{Q} \otimes_K K_\mathfrak{p}$ we define the resolvent by

$$(a \mid \chi) = \det(\sum a^\gamma T(\gamma)^{-1}).$$

This is an element of $\bar{Q}^*_{\mathfrak{p}}$ in fact of $(NE)^*_{\mathfrak{p}}$. But (cf. Fröhlich [1, Theorem 21])

$$g_{\mathfrak{p}}(\mathfrak{s}(M)) = (a|\chi)\bar{\mathfrak{o}}_{\mathfrak{p}}.$$

Hence by (2.5)

$$[(a|\chi)^{\deg(\phi)}(a|\phi)^{\deg(\chi)}(a|\chi\phi)^{-1}]\bar{\mathfrak{o}}_{\mathfrak{p}} = \mathfrak{T}(M, N)_{\mathfrak{p}}. \tag{3.1}$$

Indeed the expression in square brackets on the left lies in $E^*_{\mathfrak{p}}$. View it as an idèle. It then defines a global fractional ideal of $\bar{\mathfrak{o}}$, "localized" at primes above. Similarly $\mathfrak{T}(M, N)$ is an ideal of $\bar{\mathfrak{o}}$ localized at these primes. From (3.1) we now get, in the obvious notation, the equation

$$((a|\chi)^{\deg(\phi)}(a|\phi)^{\deg(\chi)}(a|\chi\phi)^{-1}) = \mathfrak{T}(M, N) \tag{3.2}$$

for ideals of $\bar{\mathfrak{o}}$.

The proof of Theorem 3 now follows from (3.2) and Fröhlich [1, Theorem 4], using (1.3), and the observation that if $\{\omega\}$ is a right transversal of Ω_E in $\Omega_{Q(\chi,\phi)}$, $\{\sigma\}$ one of Ω_k in Ω_Q, then $\{\omega\sigma\}$ is one of Ω_K in Ω_Q.

Similarly, the proof of Theorem 4 follows from (3.2) and Fröhlich [1, Theorem 18].

REFERENCES

[1] A. Fröhlic, Arithmetic and Galois module structure for tame extensions, *Crelle* **286/287** (1976), 380–440.

[2] A. Fröhlich, Module conductors and module resolvents, *Proc. London Math. Soc.* **32** (1976), 279–321.

[3] A. Fröhlich, Resolvents, discriminants and trace invariants, *J. Algebra* **4** (1966), 643–662.

[4] J. Martinet, Character theory and Artin *L*-functions, Algebraic Numberfields Proc. Durham Symposium, Academic Press, New York, 1977, 1–87.

AMS (MOS) 1970 subject classification: 12A99.

The Hasse Norm Theorem for l-Extensions of the Rationals

DENNIS A. GARBANATI

UNIVERSITY OF MARYLAND
COLLEGE PARK, MARYLAND

Let k be a finite abelian extension of the rationals Q. We take "the Hasse norm theorem holds for k" to mean that each nonzero rational number is the norm of an element of k if and only if it is the norm of an element from each completion of k. This paper gives computable necessary and sufficient conditions for the Hasse norm theorem to hold for k in the case where k satisfies the following properties: (i) $[k : Q]$ is a power of l where l is any prime, (ii) k is the composite of cyclic extensions of Q that have pairwise relatively prime conductors, and (iii) the conductor of k is odd.

Introduction

In 1931 H. Hasse [7] gave an example, i.e., $k = Q((-3)^{1/2}, 13^{1/2})$, that showed that the Hasse norm theorem did not hold for arbitrary abelian extensions. In 1936 A. Scholz [12] gave conditions for the Hasse norm theorem to hold for certain noncyclic extensions of degree l^2 over the ground field where l is a prime. In 1967 J. Tate and J.-P. Serre [1, p. 360] gave a method for producing numbers that were local norms everywhere but not global norms from $Q(13^{1/2}, 17^{1/2})$. In 1971 C. Pitti [11] and now O. Taussky-Todd [13] have given substitutes for the Hasse norm theorem for Klein 4-group extensions.

This paper continues the project started in Garbanati [4, 5] of classifying those abelian extensions of the rationals for which the Hasse norm theorem holds.

1. Preliminaries

We now state those results of Garbanati [5] that we shall use but not prove and we introduce some new notation.

Let k be a finite abelian extension of the rationals Q with Galois group $G(k/Q)$.

If F is a field, let F^* be the multiplicative group $F - \{0\}$.

Let p be a prime divisor (finite or infinite) of Q and let $\beta \in Q^*$. Let $(\beta, k)_p$ be the Hasse norm residue symbol (cf. Garbanati [5] for a definition). Let N be the norm map from k to Q. By an abuse of language we shall take the phrase "the Hasse norm theorem holds for k" to mean that "for any $\beta \in Q^*$ there exists a $\hat{\beta} \in k$ such that $N\hat{\beta} = \beta$ if and only if $(\beta, k)_p = 1$ for all prime divisors p of Q."

Let K' be the "narrow" genus field of k, i.e., the largest abelian extension of k that is unramified at all (finite) prime ideals of k and which is abelian over Q.

Let $\bar{K}$ be the "narrow" central class field of k, i.e., the largest abelian extension of k that is unramified at all (finite) prime ideals of k and which is a Galois extension of Q such that $G(\bar{K}/k)$ is a subset of the center of $G(\bar{K}/Q)$.

Let $g^+ = [K' : k]$ and $z^+ = [\bar{K} : k]$.

Theorem 1 *Let k be an arbitrary finite abelian extension of Q. Then the Hasse norm theorem holds for k if and only if $z^+ = g^+$.*

Proof [5, Theorem 1].

Theorem 2 *Let k_0 and k be arbitrary finite abelian extensions of Q such that $k_0 \supset k$. If the Hasse norm theorem holds for k_0, then it holds for k.*

Proof [5, Theorem 2].

Lemma 1 *Let k_0 and k be arbitrary finite abelian extensions of Q such that $k_0 \supset k$. Let $\bar{K}_0$ be defined for k_0 as $\bar{K}$ was defined for k. Then $\bar{K} \subset \bar{K}_0$.*

Proof [5].

Let $k_* = K'$. Let $\bar{K}_*$ be defined for k_* as $\bar{K}$ was defined for k. If G is a group, then let (G, G) be its commutator subgroup.

Lemma 2 *Let k be an arbitrary finite abelian extension of Q. Then $G(\bar{K}_*/k_*) = (G, G)$, where $G = G(\bar{K}_*/Q)$.*

Proof [5, Lemma 14].

Let $Q_m = Q(e^{2\pi i/m})$ where m is a positive integer and let f be the conductor of k, i.e., the smallest positive integer such that $k \subset Q_f$.

If G is a finite abelian group, let G' denote the group of characters of G. If n is a positive integer, let G_n denote the multiplicative group of integers mod n. Let $G = G(Q_f/Q)$ and $H = G(Q_f/k)$. Then $G(k/Q) = G/H$. Let $\zeta = e^{2\pi i/f}$. If $a \in Z$ (the integers) and a and f are relatively prime, let $\sigma_a\colon \zeta \to \zeta^a$ be a typical element of G. Let τ be the isomorphism of G onto G_f given via $\sigma_a \to a$. Let $H_f = \tau(H)$. Let $X = X_k$ be the group of all the characters of G'_f that take on the value 1 at each element of H_f. Let

$$f = p_1^{d_1} \cdots p_s^{d_s}$$

be the prime power decomposition of f. Since

$$G_f \simeq G_{n_1} \times \cdots \times G_{n_s}$$

where $n_i = p_i^{d_i}$ $(1 \leq i \leq s)$ we can identify the two groups above and write

$$G'_f = G'_{n_1} \times \cdots \times G'_{n_s},$$

thinking of the characters of G'_f as s-tuples of characters. For $1 \leq i \leq s$ consider the projection map

$$\mathrm{pr}_i\colon G'_f \to G'_{n_i}.$$

Let $X_i = \mathrm{pr}_i X$. Let $\tilde{X}$ be the external direct product of the X_i for $1 \leq i \leq s$, i.e.,

$$\tilde{X} = \mathrm{dir}\prod_{i=1}^{s} X_i.$$

By [8, p. 357] $\tilde{X} = X_{K'}$.

Throughout the rest of this section we shall assume that:

(I) $[k : Q]$ is a power of l where l is any prime;
(II) the conductor f of k is odd.

Let k_0 be the largest field such that $k \subset k_0 \subset Q_f$ and $[k_0 : Q]$ is a power of l. Let $X^0 = X_{k_0}$. Since p_i $(1 \leq i \leq s)$ is odd, X_i^0 is cyclic. Let χ_i^0 be a generator of X_i^0. (We shall require that χ_i^0 be a certain type of generator of X_i^0 in Section 3.) Let $o(\cdot)$ denote "the order of." Let $\alpha(i) = o(X_i^0)$. Let $\delta_i = e^{2\pi i/\alpha(i)}$. We define $[p_i, p_j]$ $(1 \leq i, j \leq s)$ by the conditions

$$0 < [p_i, p_j] \leq \alpha(i), \qquad [p_i, p_i] = \alpha(i),$$

and

$$\chi_i^0(p_j) = \delta_i^{[p_i, p_j]} \qquad \text{if} \quad j \neq i.$$

Let $I(\mathfrak{p}_i \mid p_i)$ be the inertia group of p_i where $\mathfrak{p}_i$ is some prime ideal in k_0 dividing p_i. Let $\sigma_{ik_0} \in I(\mathfrak{p}_i \mid p_i)$. (We are using σ_i instead of (p_i) which was used in [5].)

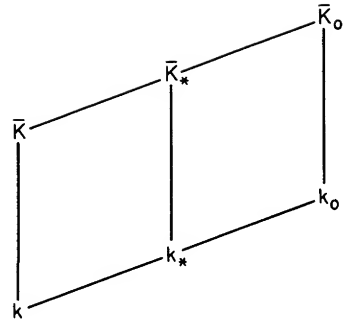


FIG. 1

Let $\bar{K}_0$ be defined for k_0 as $\bar{K}$ was defined for k. By Lemma 1 we have Fig. 1.

By Garbanati [5, Lemma 11] there exists $\sigma_{i\bar{K}_0} \in I(\mathfrak{P}_i \mid p_i)$ (the inertia group of p_i where $\mathfrak{P}_i$ is a prime ideal in $\bar{K}_0$) such that $\sigma_{i\bar{K}_0}$ restricted to k_0 is σ_{ik_0}.

Let σ_i be $\sigma_{i\bar{K}_0}$ restricted to $\bar{K}_*$.

Let $X = X_{k_*} \subset X^0 = X_{k_0}$. Let $\beta(i) = o(X_i)$. Let $\beta(i, j) = \min\{\beta(i), \beta(j)\}$.

If G is a group, let (g_1, g_2) be the commutator $g_1^{-1} g_2 g_1 g_2^{-1}$ and let cen G be the center of G.

Suppose $k_* = K'$ is noncyclic. Then for appropriately chosen σ_{ik_0} we have the following lemmas. (We shall explain how to choose σ_{ik_0} in Section 3.)

Lemma 3 *Let $G = G(\bar{K}_*/Q)$. Then G is generated by the σ_i $(1 \le i \le s)$ and $(G, G) \subset$ cen G.*

Proof [5, Lemma 13].

Lemma 4 *Let W be the free group with $\binom{s}{2}$ generators w_{ij} $(1 \le i < j \le s)$. Let N be the normal subgroup generated by the relators*

$$(w_{ij}, w_{bc}) \qquad 1 \le i < j \le s, \quad 1 \le b < c \le s \tag{1}$$

$$w_{ij}^{\beta(i,j)} \qquad 1 \le i < j \le s \tag{2}$$

$$\prod_{j<i} w_{ji}^{[p_j, p_i]} \prod_{i<j} w_{ij}^{-[p_j, p_i]} \qquad 1 \le i \le s. \tag{3}$$

(Note that i is a fixed number between 1 and s in the last type of relator.) Then

$$W/N \simeq G(\bar{K}_*/k_*)$$

via

$$w_{ij}N \to (\sigma_i, \sigma_j).$$

Proof [5, Lemma 15].

2. A Criterion for the Hasse Norm Theorem to Hold

Throughout the rest of this paper we shall define G via

$$G = G(\bar{K}_*/Q)$$

and H via

$$H = G(\bar{K}_*/k).$$

Let (G, H) be the normal subgroup of G generated by the elements by (g, h) where $g \in G$ and $h \in H$.

Lemma 5 *Let k be an arbitrary finite abelian extension of Q. Then $G(\bar{K}_*/\bar{K}) = (G, H)$.*

Proof Let $E = G(\bar{K}_*/\bar{K})$. Let $g \in G$ and $h \in H$. Then $(g, h) \in E$, i.e., $gEhE = hEgE$ because $H/E = G(\bar{K}/k) \subset \text{cen } G(\bar{K}/Q) = \text{cen } G/E$. Thus $(G, H) \subset E$. Now to show $E \subset (G, H)$. Let K be the field fixed by (G, H). Since $(G, H) \subset (G, G)$, it follows from Lemma 2 that $K \supset k_* \supset k$. Also $\bar{K}_*$ is unramified over k_*, which in turn is unramified over k. So K is unramified over k. Since $g(G, H)h(G, H) = h(G, H)g(G, H)$, we get $G(K/k) = H/(G, H) \subset \text{cen } G/(G, H) = \text{cen } G(K/Q)$. Therefore, $K \subset \bar{K}$ and so $E \subset (G, H)$.

Lemma 6 *Let k be an arbitrary finite abelian extension of Q. The Hasse norm theorem holds for k if and only if $(G, G) = (G, H)$.*

Proof By Theorem 1 the Hasse norm theorem holds if and only if $\bar{K} = k_*$ which happens if and only if $(G, H) = G(\bar{K}_*/\bar{K}) = G(\bar{K}_*/k_*) = (G, G)$.

3. The Structure of $(G, G)/(G, H)$ for Fields with Properties (I)–(IV)

In this section, for a specific type of extension of Q, we shall: (a) find a set of generators of H (Lemma 7), (b) find a set of generators for (G, H) (Lemma 8), and (c) give a matrix method for determining the invariants of $(G, G)/(G, H)$.

Throughout this section we shall assume that k is an abelian extension of

Q with the following properties:

(I) $[k : Q]$ is a power of l where l is any prime.
(II) The conductor f of k is odd.
(III) k is noncyclic.
(IV) k is the composite of cyclic fields with pairwise relatively prime conductors, i.e.,

$$k = L_1 \cdots L_t$$

where each L_d $(1 \leq d \leq t)$ is a cyclic extension of Q and if f_d and $f_{d'}$ are the conductors of L_d and $L_{d'}$, respectively, and $d \neq d'$, then f_d and $f_{d'}$ are relatively prime.

We shall now produce $X = X_k$. Let S_d $(1 \leq d \leq t)$ be defined via

$$S_d = \{i \mid 1 \leq i \leq s \text{ and } p_i \mid f_d\}.$$

Without loss of generality we may assume that the p_i $(1 \leq i \leq s)$ are ordered so that if $1 \leq d < d' \leq t$ and $i \in S_d$ and $i' \in S_{d'}$, then $i < i'$. Let ψ_d be a generator of X_{L_d}. Then

$$X_k = X_{L_1} \times \cdots \times X_{L_t} = \langle \psi_{d_1} \rangle \times \cdots \times \langle \psi_{d_t} \rangle.$$

If $i \in S_d$, let $\chi_i = \mathrm{pr}_i \psi_d$. As mentioned in Section 1, we now restrict χ_i^0, i.e., χ_i^0 must be a generator of X_i^0 having the property $(\chi_i^0)^{\alpha(i)/\beta(i)} = \chi_i$. Let $v_i = e^{2\pi i/\beta(i)}$. Then

$$\chi_i(p_j) = v_i^{[p_i, p_j]} \qquad \text{if} \quad j \neq i.$$

Let k_i be the largest subfield of Q_{n_i} such that $[k_i : Q]$ is a power of l. In Section 1 we stated that Lemmas 3 and 4 held for appropriately chosen $\sigma_{ik_0} \in I(\mathfrak{p}_i \mid p_i)$ where $\mathfrak{p}_i$ is a prime ideal in k_0. To be more precise this means σ_{ik_0} generates $I(\mathfrak{p}_i \mid p_i)$ and σ_{ik_0} satisfies the following relation for all j $(1 \leq j \leq s)$ [5; 2, p. 238]:

$$(p_j, k_i)_{(p_i)} = \sigma_{ik_0}^{[p_i, p_j]} \tag{4}$$

where $(p_i) = p_i Z$. (For this equality we are really thinking of σ_{ik_0} as restricted to k_i.) We shall now produce such a σ_{ik_0}. Let a_i' be an integer (relatively prime to n_i) such that $\chi_i^0(a_i') = \delta_i$ and hence $\chi_i(a_i') = v_i$. Let a_i be an integer such that

$$a_i \equiv a_i' \bmod n_i \qquad \text{and} \qquad a_i \equiv 1 \bmod f/n_i.$$

Then

$$\chi_i(a_i) = v_i \tag{5}$$

Let $\zeta = e^{2\pi i/f}$. Let σ_{ik_0} be the automorphism on k_0 given by restricting $\zeta \to \zeta^{a_i}$ to k_0. Then σ_{ik_0} generates $I(\mathfrak{p}_i \mid p_i)$ and for $i \neq j$ we have $\chi_i^0(a_i^{[p_i, p_j]}) = \chi_i^0(p_j)$.

Therefore if $j \neq i$, then

$$(p_j, k_i)_{(p_i)} = \left(\frac{k_i}{(p_j)}\right) = \sigma_{ik_0}^{[p_i, p_j]}.$$

where $(\div)$ is the Artin symbol. If $j = i$, then (4) holds trivially.

Let $c(d)$ $(1 \leq d \leq t)$ be an integer in S_d with the property that

$$\beta(c(d)) \geq \beta(i) \qquad \text{for all} \quad i \in S_d.$$

If $i \in S_d$, let

$$\mu(i) = \beta(c(d))/\beta(i).$$

(Note that i determines d.) If $i \in S_d$, let

$$\tau_i = \sigma_{c(d)}^{\mu(i)} \sigma_i^{-1}.$$

Lemma 7 *The automorphisms* τ_i $(1 \leq i \leq s)$ *and the elements of* (G, G) *generate* H.

Proof Since $k_* \supset k$, we get by Lemma 2 that $(G, C) \subset H$. We now show $\tau_i \in H$ where $i \in S_d$. For this proof, let $b_i = a_{c(d)}^{\mu(i)}$. Then τ_i restricted to k is $\zeta \to \zeta^{b_i a_i^{-1}}$ restricted to k where a_i^{-1} is the multiplicative inverse of a_i in the integers mod f. But by (5) we get

$$\psi_d(b_i a_i^{-1}) = \chi_{c(d)}(a_{c(d)}^{\mu(i)}) \chi_i(a_i)^{-1} = v_{c(d)}^{\mu(i)} v_i^{-1} = 1.$$

Thus $\tau_i \in H$.

Now we need only show that any automorphism in H can be written as a product composed of the τ_i and elements of (G, G). Let $h \in H$. Since $h \in G$, it follows from Lemma 3 that

$$h = h_1 \cdots h_t g$$

where $g \in (G, G)$ and for $1 \leq d \leq t$

$$h_d = \prod_{i \in S_d} \sigma_i^{-e_i}.$$

Let all products which follow in this proof run over all $i \in S_d$. Since $h \in H$ we get h_d fixes L_d. Furthermore, h_d restricted to L_d is $\zeta \to \zeta^{m(d)}$ restricted to L_d where $m(d) = \prod a_i^{-e_i}$. Thus

$$1 = \psi_d(m(d)^{-1}) = \prod \chi_i(a_i)^{e_i} = \prod \chi_{c(d)}(b_i)^{e_i} = \chi_{c(d)}(\prod b_i^{e_i}).$$

Therefore $\zeta \to \zeta^{n(d)}$ restricted to k_* is 1 where $n(d) = \prod b_i^{e_i}$. Thus $\prod \sigma_{c(d)}^{\mu(i)e_i}$ restricted to k_* is 1, i.e., $\prod \sigma_{c(d)}^{\mu(i)e_i} \in (G, G)$. So we have

$$h_d(G, G) = \prod \sigma_{c(d)}^{\mu(i)e_i} \sigma_i^{-e_i}(G, G) = \prod \tau_i^{e_i}(G, G).$$

Before proving the next lemma we note that if a, b, and c are elements of

some group E and $(E, E) \subset \operatorname{cen} E$, then

$$(a, bc) = (a, b)(a, c) \quad \text{and} \quad (ab, c) = (a, c)(b, c) \tag{6}$$

$$(a, b^{-1}) = (a, b)^{-1} \tag{7}$$

$$(a, b) = (b, a)^{-1}. \tag{8}$$

Lemma 8 *The following elements generate* (G, H)*:*

$$(\sigma_{c(d)}, \sigma_{c(d')})^{\mu(i)\mu(i')}(\sigma_i, \sigma_{i'})^{-1} \tag{9}$$

where $i \in S_d$ *and* $i' \in S_{d'}$ *and* $1 \leq d \leq d' \leq t$ *and* $i < i'$*. Note that if* $d = d'$*, then* (9) *reduces to* $(\sigma_i, \sigma_{i'})^{-1}$*.*

Proof We first show that an element of the type (9) is in (G, H). By (6), (7), and Lemma 7

$$(\sigma_{c(d)}, \sigma_{c(d')})^{\mu(i')}(\sigma_{c(d)}, \sigma_{i'})^{-1} = (\sigma_{c(d)}, \tau_{i'}) \in (G, H). \tag{10}$$

Similarly,

$$(\sigma_{i'}, \sigma_{c(d)})^{\mu(i)}(\sigma_{i'}, \sigma_i)^{-1} \in (G, H) \tag{11}$$

Therefore by (8), (10), and (11) elements of type (9) are in (G, H).

Now we show each element of (G, H) is a product of powers of elements of type (9). By (6) and Lemmas 3 and 7, (G, H) is generated by $(\sigma_i, \tau_{i'})$ where $1 \leq i, i' \leq s$. Suppose $i \leq i'$. Then

$$\begin{aligned}(\sigma_i, \tau_{i'}) &= (\sigma_i, \sigma_{c(d')})^{\mu(i')}(\sigma_i, \sigma_{i'})^{-1} \\ &= [(\sigma_{c(d)}, \sigma_{c(d')})^{\mu(i)}(\sigma_i, \sigma_{c(d')})^{-1}]^{-\mu(i')} \\ &\quad \times [(\sigma_{c(d)}, \sigma_{c(d')})^{\mu(i)\mu(i')}(\sigma_i, \sigma_{i'})^{-1}],\end{aligned}$$

If $i \leq c(d')$, then each element in the brackets is either of type (9) or is 1. If $i > c(d')$, then $d = d'$ and the first component above can be written as $(\sigma_{c(d')}, \sigma_i)^{-\mu(i')}$ which is a power of an element of type (9). Suppose $i > i'$. Applying (8) to the right-hand side of the above shows $(\sigma_i, \tau_{i'})$ is a product of powers of elements of type (9).

Lemma 9 *Let* k *satisfy* (I)–(IV)*. Let* W *be the free group with* $\binom{s}{2}$ *generators* w_{ij}, $1 \leq i < j \leq s$*. Let* R *be the normal subgroup generated by the relators given in* (1), (2), *and* (3) *and by*

$$w_{c(d)c(d')}^{\mu(i)\mu(i')} w_{ii'}^{-1} \tag{12}$$

where $i \in S_d$, $i' \in S_{d'}$, *and* $1 \leq d \leq d' \leq t$ *and* $i < i'$*. Then* $W/R \simeq (G, G)/(G, H)$*.*

Proof This follows from Magnus *et al.* [9, p. 71] and Lemmas 4 and 8.

We shall now produce a matrix procedure for computing the invariants

of $(G, G)/(G, H)$. Let $r = \binom{s}{2}$. Order (i, j), $1 \leq i < j \leq s$, lexicographically, i.e.,

$$(1, 2), (1, 3), \ldots, (1, s), (2, 3), \ldots, (2, s), \ldots, (s-1, s) \tag{13}$$

Let this ordering determine the position of the entries in the following matrices.

Let A be the $r \times r$ diagonal matrix $A = \operatorname{diag}[\beta(i, j)]$ where using the ordering of (13) $\beta(i, j)$ is in the (i, j)th row and column.

Let B be the $s \times r$ matrix where the ith row is obtained from (3) as follows. Let $1 \leq j \leq s, j \neq i$. If $j < i$, put $[p_j, p_i]$ in the (j, i)th column. If $i < j$, put $-[p_j, p_i]$ in the (i, j)th column. Put zero elsewhere in the ith row.

Let E be the $r \times r$ matrix where the (i, i')th row is obtained from (12) as follows. Let $i \in S_d$ and $i' \in S_{d'}$. If $d = d'$, then put 1 in the (i, i')th column and put zeros elsewhere in the (i, i')th row. Suppose $d \neq d'$. If $(i, i') = (c(d), c(d'))$, put zeros everywhere in the (i, i')th row. If $(i, i') \neq (c(d), c(d'))$, put $\mu(i)\mu(i')$ in the $(c(d), c(d'))$th column and put -1 in the (i, i')th column. Put zeros elsewhere in the (i, i')th row. Let 0_1 be the $r \times (s + r)$ zero matrix and 0_2 the $s \times (s + r)$ zero matrix. Let $m = 2r + s$. Let M be the $m \times m$ matrix

$$M = \begin{bmatrix} A & 0_1 \\ B & 0_2 \\ E & 0_1 \end{bmatrix}.$$

The Smith normal form of an $m \times m$ matrix M over Z is the unique matrix that results from applying elementary row and column operations to M so as to obtain an $m \times m$ diagonal matrix

$$\operatorname{diag}(z_1, \ldots, z_c, 0, \ldots, 0)$$

where $z_i \mid z_{i+1}$ for $1 \leq i \leq c - 1$ and each z_i is a positive integer [10, p. 26]. The $z_1, \ldots, z_c$ are the invariant factors of M.

Theorem 3 *Let k satisfy* (I)–(IV). *Let M be the $m \times m$ matrix described above. Then there are precisely r invariant factors of M, namely, $z_1, \ldots, z_r$. Suppose $z_1 = \cdots = z_e = 1$ and $z_{e+1} \neq 1$. Then $z_{e+1}, \ldots, z_r$ are the invariants of $(G, G)/(G, H) \simeq G(\bar{K}/K')$.*

Proof The same proof as was given in Garbanati [5, Theorem 11] works if we replace $A/A^{\Delta}R$ by $(G, G)/(G, H)$.

If $b \in Z$, let $\bar{b}$ be b mod l. If C is a matrix over Z, let $\bar{C}$ be the matrix over F_l (the Galois field with l elements) obtained by replacing each entry b of E with $\bar{b}$.

Let $C = \left[\begin{smallmatrix} B \\ E \end{smallmatrix}\right]$.

Corollary 1 *Let k satisfy* (I)–(IV). *Then $(G, G)/(G, H)$ is the trivial group if and only if rank $\bar{C} = r$.*

Proof Let U_1 and U_2 be unimodular matrices such that $U_1 M U_2 =$

$\operatorname{diag}(z_1, \ldots, z_r) \dot{+} 0_3$ where 0_3 is the $(s+r) \times (s+r)$ zero matrix. Then $(G, G)/(G, H)$ is trivial $\Leftrightarrow e = r \Leftrightarrow \operatorname{rank} \bar{U}_1 \bar{M} \bar{U}_2 = r \Leftrightarrow \operatorname{rank} \bar{C} = r$.

4. The Hasse Norm Theorem for Fields with Properties (I)–(IV)

In the following theorem we find a new matrix D over F_l such that $\operatorname{rank} D = \binom{t}{2}$ if and only if $\operatorname{rank} \bar{C} = r$ and then we use Lemma 6 and Corollary 1 to give a necessary and sufficient condition for the Hasse norm theorem to hold for k in terms of the rank of D.

We now define D. Let k satisfy (I)–(IV). In particular

$$k = L_1 \cdots L_t$$

is the composite of t cyclic extensions of Q (namely, L_d $(1 \leq d \leq t)$) which have pairwise relatively prime conductors. Let $S = \{p_1, \ldots, p_q\}$ be those primes which ramify totally in some L_d $(1 \leq d \leq t)$. Note we are not fixing d here, i.e., perhaps p_1 ramifies totally in L_d and p_2 ramifies totally in $L_{d'}$ where $d \neq d'$. Let ψ_d generate X_{L_d}, i.e.,

$$X_{L_d} = \langle \psi_d \rangle$$

where X_{L_d} is the character group associated with L_d. Let $a_d = [L_d : Q]/l$. Let $\omega = e^{2\pi i/l}$. Let f_d be the conductor of L_d. Let

$$S_d = \{j \mid p_j \in S \text{ and } p_j \mid f_d\}.$$

If $p_j \in S$ but $j \notin S_d$, define a_{dj} $(0 < a_{dj} \leq l)$ via

$$\psi_d^{a_d}(p_j) = \omega^{a_{dj}}.$$

Let $u = \binom{t}{2}$. Order the u pairs (d, d') where $1 \leq d < d' \leq t$ lexicographically (cf. (13)) and use this ordering for the columns of the following $q \times u$ matrix D (over F_l). The jth row of D is determined as follows. If $j \in S_d$ and $1 \leq d < d' \leq t$, put $-\bar{a}_{d'j}$ in the (d, d')th column. If $j \in S_{d'}$ and $1 \leq d < d' \leq t$, put $\bar{a}_{dj}$ in the (d, d')th column. Put zeros elsewhere in the jth row.

Theorem 4 *Let k satisfy* (I)–(IV). *Let D be the matrix over F_l defined above. Then the Hasse norm theorem holds for k if and only if* $\operatorname{rank} D = u$.

Proof We shall show that

$$\operatorname{rank} D = u \Leftrightarrow \operatorname{rank} \bar{C} = r \tag{14}$$

and then the theorem will follow from Lemma 6 and Corollary 1. We shall now prove (14) by performing a series of row and column operations on C and then simplifying and analyzing the matrix that results. In what follows let ERO (resp. ECO) stand for elementary row (resp. column) operation.

Consider the E part of C. We use the notation employed to define E. For

the (i, i')th row of E, there are two cases. Either $d = d'$ or $d \neq d'$. If $d = d'$, then use the 1 in the (i, i')th row and column of E to change (via ERO) all other entries in the (i, i')th column of C to 0. If $d \neq d'$ and $(i, i') \neq (c(d), c(d'))$, change the i'th row of B as follows. Multiply the (i, i')th row of E by $[p_i, p_{i'}]$ and add the resulting row to the i'th row of B. Also change the ith row of B as follows. Multiply the (i, i')th row of E by $-[p_{i'}, p_i]$ and add to the ith row of B. At this point if $(i, i') \neq (c(d), c(d'))$ and $d \neq d'$ the (i, i')th column of C will contain -1 in the (i, i')th row of E of C and zeros elsewhere. Use this -1 (via ECO) to change to 0 the $\mu(i)\mu(i')$ in the (i, i')th row and $(c(d), c(d'))$th column of E. Now change this -1 to $+1$ (via ERO). Change the $(c(d), c(d'))$ column (via ECO) into a (d, d') column, i.e., move it to the (d, d') column position. Since $1 \leq d < d' \leq t$, there are u pairs (d, d'). We have now transformed C into the direct sum of two matrices B_0 and E_0, i.e., $C = B_0 \dot{+} E_0$ where B_0 is an $s \times u$ matrix and E_0 is an $r \times (r - u)$ matrix. But E_0 can be transformed (via EROs and ECOs) into $\begin{bmatrix} I_{r-u} \\ 0 \end{bmatrix}$ where I_{r-u} is the $(r - u) \times (r - u)$ identity matrix and 0 is the $u \times (r - u)$ zero matrix. We now have

$$\text{rank } \bar{C} = r \Leftrightarrow \text{rank } \bar{B}_0 = u. \tag{15}$$

What does the jth row of B_0 look like? If $j \in S_{d'}$, then in the (d, d')th column $(d < d')$ we have

$$\sum_{i \in S_d} \mu(i)\mu(j)[p_i, p_j]. \tag{16}$$

If $j \in S_d$, then in the (d, d')th column $(d < d')$ we have

$$\sum_{i' \in S_{d'}} -\mu(j)\mu(i')[p_{i'}, p_j]. \tag{17}$$

If $j \notin S_d \cup S_{d'}$, then we have 0 in the (d, d')th column.

Let $j \in S_h$ where $1 \leq h \leq t$, i.e., $p_j \mid f_h$. Since the ramification index of p_j in L_h is $o(\chi_j) = \beta(j)$ [8, p. 358] and since $[L_h : Q] = o(X_{L_h}) = \beta(c(h))$, we get that p_j ramifies totally in the cyclic field L_h if and only if $\beta(c(h)) = \beta(j)$ if and only if $l \nmid \mu(j)$.

Consider $\bar{B}_0$. If p_j does not ramify totally in L_h where $j \in S_h$, then by (16) and (17) the jth row of $\bar{B}_0$ is the zero vector. If p_j ramifies totally in L_h where $j \in S_h$ (i.e., $\mu(j) = 1$), and if $j \notin S_d$, then

$$\psi_d(p_j) = \prod \chi_i(p_j) = \prod v_i^{[p_i, p_j]} = \prod v_{c(d)}^{\mu(i)[p_i, p_j]}$$

where these products and the product that follows run over all $i \in S_d$. Let $a_d = \beta(c(d))/l$. Then $v_{c(d)}^{a_d} = \omega$ where $\omega = e^{2\pi i/l}$. Thus

$$\psi_d(p_j)^{a_d} = \prod \omega^{\mu(i)[p_i, p_j]}. \tag{18}$$

If $j \notin S_d$, define a_{dj} $(0 < a_{dj} \leq l)$ via

$$\psi^{a_{dj}}(p_j) = \omega^{a_{dj}}. \tag{19}$$

By (18) and (19)

$$a_{dj} \equiv \sum_{i \in S_d} \mu(i)[p_i, p_j] \bmod l. \tag{20}$$

By (20) $\bar{B}_0$ is in fact the $s \times u$ matrix given by the following prescription for the jth row. If p_j does not ramify totally in L_h where $j \in S_h$, then let the jth row be the zero vector. By (16), (17), and (20) we have the following. If p_j ramifies totally in $L_{d'}$ where $j \in S_{d'}$, then in the (d, d')th column $(d < d')$ we have $\bar{a}_{dj}$. If p_j ramifies totally in L_d where $j \in S_d$, then in the (d, d')th column we have $-\bar{a}_{d'j}$. If p_j ramifies totally in L_h where $j \in S_h$ but $j \notin S_d \cup S_{d'}$, then we have 0 in the (d, d')th column. Hence rank $\bar{B}_0$ = rank D and we are done, i.e., (14) now follows from (15).

Let T be the set of all p_j $(1 \leq j \leq s)$ that ramify totally in L_c for some c $(1 \leq c \leq t)$ (i.e., $p_j \in S$) and which, in addition, split in L_d for all $d \neq c$. Let $\#(\cdot)$ stand for "the number of elements in."

Theorem 5 *Let k satisfy* (I)–(IV). *If $q - \#(T) < u$, then the Hasse norm theorem does not hold for k.*

Proof If $p_j \in T$, then $p_j \in S$ and so p_j determines a row in D. Let g_j be the number of primes in L_d that divide p_j. Then g_j is the order of the set of all $\chi \in X_{L_d}$ such that p_j does not divide the conductor of χ and simultaneously $\chi(p_j) = 1$ [8, p. 356]. Therefore since p_j splits in each L_d where $d \neq c$, we have $\psi_d^{a_d}(p_j) = 1$ for all $d \neq c$. Therefore the row determined by p_j is the zero row and so there are at most $q - \#(T)$ nonzero rows in D. The result now follows from Theorem 4.

The following theorem generalizes Garbanati [5, Theorem 10].

Theorem 6 *Let k satisfy* (I)–(IV). *Let k be the composite of t cyclic extensions of Q, namely L_d $(1 \leq d \leq t)$, which have pairwise relatively prime conductors. Let q be the number of primes that ramify totally in some L_d $(1 \leq d \leq t)$. If $q < \binom{t}{2}$, the Hasse norm theorem does not hold.*

Proof This is immediate from Theorem 4.

Example Let $p_1, \ldots, p_5$ be distinct odd primes. Let

$$k = Q((\varepsilon_1 p_1 p_2)^{1/2}, (\varepsilon_2 p_3)^{1/2}, (\varepsilon_3 p_4)^{1/2}, (\varepsilon_4 p_5)^{1/2})$$

where $\varepsilon_i = \pm 1$ $(1 \leq i \leq 4)$ and $\varepsilon_1 p_1 p_2 \equiv 1 \bmod 4$, $\varepsilon_i p_{i+1} \equiv 1 \bmod 4$ $(2 \leq i \leq 4)$. Then k satisfies (I)–(IV). Since $q = 5$ and $u = 6$, the Hasse norm theorem does not hold for k.

Corollary 2 *Let k satisfy* (I)–(IV). *Let k be the composite of four or more*

cyclic extensions L_d of Q that have pairwise relatively prime conductors. If precisely one prime ramifies totally in each L_d, then the Hasse norm theorem does not hold for k.

Proof In this case $q = t \geq 4$, but then $q < \binom{t}{2}$.

The following theorem generalizes Garbanati [5, Theorem 8].

Theorem 7 *Let k satisfy* (I)–(II). *Let $k = L_1 \cdot L_2$ be the composite of two cyclic extensions of Q (namely L_1 and L_2) that have relatively prime conductors. Then the Hasse norm theorem holds if and only if there exists a prime $p \in Q$ that ramifies totally in either L_1 or L_2 and at the same time does not split in k (i.e., only one prime in k divides p).*

Proof Let $p_1, \ldots, p_q$ be the primes that ramify totally in either L_1 or L_2. We can assume $p_1, \ldots, p_n$ ramify totally in L_1 and $p_{n+1}, \ldots, p_q$ ramify totally in L_2. Then D is the transpose of the matrix

$$[-\bar{a}_{21} - \bar{a}_{22} \cdots -\bar{a}_{2n} \quad \bar{a}_{1n+1} \cdots \bar{a}_{1q}].$$

By Theorem 4 the Hasse norm theorem holds if and only if one of the entries is not zero, i.e., either $\psi_2^{a_2}(p_j) \neq 1$ for some j where $1 \leq j \leq n$ or $\psi_1^{a_1}(p_j) \neq 1$ for some j where $n + 1 \leq j \leq q$ and where $a_d = [L_d : Q]/l$ $(1 \leq d \leq 2)$. Let g_j be the number of primes in k that divide p_j. As in the proof of Theorem 5 it follows from Leopoldt [8, p. 356] that if $1 \leq j \leq n$, then $g_j = 1$ if and only if $\psi_2^{a_2}(p_j) \neq 1$. If $n + 1 \leq j \leq q$, then $g_j = 1$ if and only if $\psi_1^{a_1}(p_j) \neq 1$. The result now follows.

Such a theorem produces numerous examples where the Hasse norm theorem holds in the noncyclic case.

Example Let $k = Q((mp_1)^{1/2}, p_2^{1/2})$ where p_1 and p_2 are distinct primes and where m is an integer not divisible by p_1 or p_2. Suppose $mp_1 \equiv 1 \bmod 4$ and $p_2 \equiv 1 \bmod 4$. If $(p_1/p_2) = -1$, the Hasse norm theorem holds for k (where $(\div)$ is the Legendre symbol). This is because p_1 does not split in k if and only if $(p_1/p_2) = -1$.

Corollary 3 *Let k satisfy* (I)–(IV). *Using the notation of Theorem 6 let $k = L_1 \cdot L_2$ and suppose $[L_i : Q] = l$ for $i = 1, 2$. The Hasse norm theorem holds for k if and only if there is a prime dividing the conductor of k that does not split in k.*

For more information pertaining to this corollary, see A. Scholz [12].

Theorem 8 *Let k satisfy* (I)–(IV). *By* (IV) *$k = L_1 \cdots L_t$. If for some pair $\{L_i, L_j\}$ where $1 \leq i < j \leq t$ we have that each prime p that ramifies totally in either L_i or L_j splits in the composite $L_i \cdot L_j$, then the Hasse norm theorem does not hold for k.*

Proof This is immediate from Theorems 2 and 7.

Theorem 9 *Let k satisfy* (I)–(IV). *Using the notation of* (IV) *suppose $k = L_1 \cdot L_2 \cdot L_3$. Let $q = 3$. If for some i where $1 \leq i \leq 3$ we have for all $j \neq i$ that p_j splits in L_i, then the Hasse norm theorem does not hold for k.*

Proof Since in this case

$$\det D = \bar{a}_{31}\bar{a}_{12}\bar{a}_{23} - \bar{a}_{21}\bar{a}_{32}\bar{a}_{13}$$

it follows (as in the proof of Theorem 5) from [8, p. 356] that under the hypotheses of the theorem $\det D = 0$.

REFERENCES

[1] J. W. S. Cassels and A. Fröhlich, "Algebraic Number Theory." Thompson, Washington, D.C., 1967.

[2] A. Fröhlich, On fields of class two, *Proc. London Math. Soc.* **4** (1954), 235–256.

[3] A. Fröhlich, On the absolute class groups of abelian fields, *J. London Math. Soc.* **29** (1954), 211–217.

[4] D. Garbanati, Extensions of the Hasse norm theorem, *Bull. Amer. Math. Soc.* **81** (1975), 583–586.

[5] D. Garbanati, The Hasse norm theorem for non-cyclic extensions of the rationals, *Proc. London Math. Soc.*, to appear.

[6] H. Hasse, "Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper," 3 auflage, II. Physica-Verlag, Würzburg, 1970.

[7] H. Hasse, Beweis eines Satzes und Widerlegung einer Vermutung über das allegemeine Normenrestsymbol, *Nachr. Ges. Wiss.* **1** (1931), 64–69.

[8] H. Leopoldt, Zur Geschlectertheorie in Abelschen Zahlkörpern, *Math. Nachr.* **9** (1953), 351–362.

[9] W. Magnus, A. Karrass, and D. Solitar, "Combinatorial Group Theory." Wiley (Interscience), New York, 1966.

[10] M. Newman, "Integral Matrices." Academic Press, New York, 1972.

[11] C. Pitti, Etude des normes dans les extensions à groupe de Klein, *C. R. Acad. Sci. Paris* Sér. A **274** (1972), 1433–1435.

[12] A. Scholz, Totale Normenreste, die keine Normensind als Erzenger nicht-abelscher Körpererweiterungen I, *J. Reine Angew. Math.* **175** (1936), 100–107.

[13] O. Taussky-Todd, Additive commutators of rational 2×2 matrices, *J. Linear Algebra*, to appear.

AMS (MOS) 1970 subject classifications: 12A65, 12A50.

Scalar Extensions of Binary Lattices

ROBERT GOLD *PAUL PONOMAREV*

THE OHIO STATE UNIVERSITY
COLUMBUS, OHIO

For an algebraic number field E, let $\mathcal{O}_E$ denote the ring of integers of E and U_E the units of $\mathcal{O}_E$. Let K be an imaginary quadratic number field, $K = \mathbf{Q}(\sqrt{-D})$, where D is a positive square-free integer. Let F be a totally real extension of $\mathbf{Q}$ and $L = KF$ the compositum of K and F. In this paper we consider the following two types of scalar extensions of binary lattices in K.

First, if $\mathfrak{A}$ is a fractional ideal of K, we can form the fractional ideal $\mathfrak{A}\mathcal{O}_L$ of L.

Second, suppose $\mathfrak{L}$ is a lattice in a definite binary quadratic space V over $\mathbf{Q}$ having discriminant $-D$ (modulo squares). Then V is similar to the quadratic space K with quadratic form $n(x) = xx^J$, where J is the complex conjugation automorphism of K (cf. [1, §5.1]). Hence we may identify V with a quadratic space having underlying space K and quadratic form $c \cdot n$ for a suitable rational number c. We can form the tensor product $\tilde{\mathfrak{L}} = \mathfrak{L} \otimes_{\mathbf{Z}} \mathcal{O}_F$. Then $\tilde{\mathfrak{L}}$ may be regarded as an $\mathcal{O}_F$-submodule of L, but it need not be a fractional ideal of L, even if $\mathfrak{L}$ is a fractional ideal of K.

For each type of scalar extension, we have an appropriate notion of equivalence. In the first case it is the usual equivalence $\sim$ of fractional

ideals; in the second it is isometry between quadratic lattices. In this paper we present two theorems on the behavior of these equivalences with respect to the corresponding types of scalar extension. The first theorem generalizes a result of Kitaoka [3, Corollary to Theorem 2]. The second is the binary case of Theorem 2 in Kitaoka [3]. Our method is Galois-theoretic, and as such, differs completely from Kitaoka's, which relies on a study of the minima of positive definite lattices upon totally real extension.

Let the group of roots of unity in L be denoted by $\mathscr{W}$. If F is a Galois extension of $\mathbf{Q}$, we shall identify $\mathrm{Gal}(L/K)$ with $\mathrm{Gal}(F/\mathbf{Q})$ and denote it by G. Since J commutes with all complex embeddings of F, ε^{1-J} is a root of unity for any unit ε of L (cf. [2, p. 53]). Denote the subgroup of all roots of unity in L of this form by $\mathscr{V}$. Let $v = \mathrm{card}(\mathscr{V})$, $w = \mathrm{card}(\mathscr{W})$. Since $\mathscr{V}$ contains all squares of elements in $\mathscr{W}$, we have either $w = v$ or $w = 2v$.

Lemma 1 *Suppose F is Galois over $\mathbf{Q}$. Let $\mathfrak{A}$ be a fractional ideal of K such that $\mathfrak{A}\mathcal{O}_L$ is principal. Then $\mathfrak{A}^v \sim \mathfrak{P}_1 \cdots \mathfrak{P}_s$, where the $\mathfrak{P}_i$, $i = 1, \ldots, s$, are distinct primes of K that ramify over $\mathbf{Q}$.*

Proof By assumption, $\mathfrak{A}\mathcal{O}_L = \alpha\mathcal{O}_L$, $\alpha \in L$. For each $\sigma \in G$ we have $\alpha^\sigma\mathcal{O}_L = (\mathfrak{A}\mathcal{O}_L)^\sigma = \mathfrak{A}\mathcal{O}_L = \alpha\mathcal{O}_L$, from which it follows that $\alpha^{1-\sigma} = \varepsilon$, $\varepsilon \in U_L$. Then $(\alpha^{1-J})^{1-\sigma} = \varepsilon^{1-J}$, $\varepsilon^{1-J} \in \mathscr{V}$. Putting $\beta = \alpha^v$, $\mathfrak{B} = \mathfrak{A}^v$, we see that $(\beta^{1-J})^{1-\sigma} = 1$, so that $(\beta^{1-J})^\sigma = \beta^{1-J}$ for all $\sigma \in G$. It follows that $\beta^{1-J} \in K$ and $\mathfrak{B}^{1-J} = \beta^{1-J}\mathcal{O}_K$. Thus $\mathfrak{B} \sim \mathfrak{B}^J$, which implies $\mathfrak{B} \sim \mathfrak{P}_1 \cdots \mathfrak{P}_s$, where the $\mathfrak{P}_i$, $i = 1, \ldots, s$, are distinct primes of K ramified over $\mathbf{Q}$.

Lemma 2 *Let $\mathcal{O}$ be an order of K (not necessarily maximal). Then $\tilde{\mathcal{O}} \cap U_L = U_F$ except if $\mathcal{O} = \mathcal{O}_K$ when $D = 1, 3$.*

Proof We can write $\mathcal{O} = \mathbf{Z} \cdot 1 + \mathbf{Z} \cdot fw$, where f is a positive integer and $w = \sqrt{-D}$ or $w = (1 + \sqrt{-D})/2$, according as $-D \equiv 2, 3 \pmod 4$ or $-D \equiv 1 \pmod 4$, respectively. Suppose first that $w = \sqrt{-D}$ and $\varepsilon \in \tilde{\mathcal{O}} \cap U_L$. Write $\varepsilon = a + bf\sqrt{-D}$, $a, b \in \mathcal{O}_F$. Assume $\varepsilon \notin F$. Then $\varepsilon - \varepsilon^J = 2bf\sqrt{-D}$, so that $(1 - \varepsilon^{J-1})\mathcal{O}_L = (\varepsilon - \varepsilon^J)\mathcal{O}_L = (2bf\sqrt{-D})\mathcal{O}_L$. Now $\varepsilon^{J-1} = \zeta$, a root of unity, say a primitive mth root of unity. Then

$$(1 - \zeta)\mathcal{O}_L = (2bf\sqrt{-D})\mathcal{O}_L . \tag{1}$$

If m is not a prime power, then $1 - \zeta$ is a unit [4, p. 267], contradicting the fact that 2 divides the right-hand side of (1). Hence $m = p^t$, p a prime. Since 2 divides the right-hand side of (1), $p = 2$. But then

$$(1 - \zeta)^{\varphi(2^t)}\mathcal{O}_L = 2\mathcal{O}_L ,$$

where φ is the Euler function. Hence $\varphi(2^t) = 1$, $t = 1$. Then $b \in U_F$, $f = 1$, $D = 1$, which implies $\zeta = -1$, $\varepsilon = b\sqrt{-1}$, $\mathcal{O} = \mathcal{O}_K$.

Suppose now that $w = (1 + \sqrt{-D})/2$ and $\varepsilon \in \tilde{\mathcal{O}} \cap U_L$, $\varepsilon \in U_F$. If $\varepsilon = a + bfw$, then

$$(1 - \zeta)\mathcal{O}_L = (bf\sqrt{-D})\mathcal{O}_L, \tag{2}$$

where again $\zeta = \varepsilon^{J-1}$, a primitive mth root of unity. Since $D \equiv 3 \pmod 4$, the right-hand side of (2) $\neq \mathcal{O}_L$, so $m = p^t$, p a prime, and

$$(1 - \zeta)^{\varphi(p^t)}\mathcal{O}_L = p\mathcal{O}_L.$$

It follows that p is the only rational prime which can divide D. Hence $D = p$, $b \in U_F$, $f = 1$. Furthermore, $\varphi(p^t) = (p-1)p^{t-1} = 2$, which implies $p = 3$, $t = 1$. Thus $\zeta = (-1 \pm \sqrt{-3})/2$, $\varepsilon = b\zeta$, and $\mathcal{O} = \mathcal{O}_K$, completing the proof.

Theorem 1 *Let F be a totally real Galois extension of $\mathbf{Q}$ such that v is relatively prime to $[F : \mathbf{Q}]$. Let $\mathfrak{A}$ be a nonprincipal ideal of K. Then $\mathfrak{A}\mathcal{O}_L$ is principal if and only if there exist distinct primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ of K ramified over $\mathbf{Q}$, $\mathfrak{P}_i^2 = p_i\mathcal{O}_K$ for rational primes p_i, $i = 1, \ldots, s$, and an element $\alpha \in F$, such that*

$$\mathfrak{A} \sim \mathfrak{P}_1 \cdots \mathfrak{P}_s, \qquad (\alpha^2)\mathcal{O}_F = (p_1 \cdots p_s)\mathcal{O}_F.$$

In this case, the class of $\mathfrak{A}$ has order 2 and $p_1, \ldots, p_s$ ramify in both K and F.

Proof We need to prove the "only if" part of the statement, as the other is trivial. By Lemma 1 we know $\mathfrak{A}^v \sim \mathfrak{P}_1 \cdots \mathfrak{P}_s$ for distinct primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ of K ramified over $\mathbf{Q}$. If $\mathfrak{A}\mathcal{O}_L$ is principal, then $\mathfrak{A}^m \sim \mathcal{O}_K$, where $m = [L : K] = [F : \mathbf{Q}]$. Since $(m, v) = 1$, we have $\mathfrak{A} \sim \mathfrak{A}^{vn} \sim (\mathfrak{P}_1 \cdots \mathfrak{P}_s)^n$ for some integer n. By assumption, $\mathfrak{A}$ is nonprincipal, so n, v must both be odd, and we must have $\mathfrak{A} \sim \mathfrak{A}^v \sim \mathfrak{P}_1 \cdots \mathfrak{P}_s$. We may assume that $\mathfrak{A} = \mathfrak{P}_1 \cdots \mathfrak{P}_s$. Then $\mathfrak{A}^v = (p_1 \cdots p_s)^l \mathfrak{P}_1 \cdots \mathfrak{P}_s$, where $l = (v-1)/2$. From the proof of Lemma 1, we have $\mathfrak{A}^v = \beta\mathcal{O}_K$, where $\beta^{1-J} \in K$. But $(\mathfrak{A}^v)^{1-J} = \mathcal{O}_K$, so $\beta^{1-J} \in U_K$. Since K has class number > 1, $U_K = \{\pm 1\}$. Thus $\beta^J = \pm\beta$. If $\beta^J = \beta$, take $\alpha = (p_1 \cdots p_s)^{-l}\beta$. If $\beta^J = -\beta$, take $\alpha = c\sqrt{-D}\,\beta$ where $c \in \mathbf{Q}$ is chosen so that α^2 is square-free.

Remark The assumption on v in the statement of Theorem 1 is necessary. This can be seen by means of the following example. Let $K = \mathbf{Q}(\sqrt{-23})$, a field of class number 3. Consider the cubic extension $E = \mathbf{Q}(a)$, where $4a^3 - 9a - 2 = 0$. Since the discriminant of the latter polynomial is $144 \cdot 69$, E is totally real and its normal closure F is given by $F = E(\sqrt{69})$. Note that $L = KF$ contains a primitive cube root of unity. Put $\alpha = a + b\sqrt{-23}$, where $b = (4a^2 - 3)^{-1}$. One easily checks that $\alpha^3 = 2 + \sqrt{-23}$. Put $\mathfrak{A}$ = the fractional ideal of K generated by 3 and $(1 - \sqrt{-23})/2$. Then $\mathfrak{A}^3 = (2 + \sqrt{-23})\mathcal{O}_K$, so $\mathfrak{A}$ represents an ideal class of order 3 and $\mathfrak{A}\mathcal{O}_L = \alpha\mathcal{O}_L$. Observe that in this case $w = 6 = [F : \mathbf{Q}]$, which implies $(v, [F : \mathbf{Q}]) > 1$.

Corollary 1 (Kitaoka [3]) *Let F be a totally real extension of $\mathbf{Q}$ with discriminant relatively prime to that of K. Then every nonprincipal ideal of K remains nonprincipal in L.*

Proof The discriminant of the normal closure of F must also be relatively prime to that of K. Hence we may assume that F is Galois over $\mathbf{Q}$. If K has a nonprincipal ideal, then $D \neq 1, 3$, which implies, by Lemma 2, that $\tilde{\mathcal{O}}_K \cap U_L = U_F$. However, since K, F have relatively prime discriminants, $\tilde{\mathcal{O}}_K = \mathcal{O}_L$. Thus $U_L = U_F$, $v = 1$, and Theorem 1 is applicable. As there are no primes ramifying in both K and F, every nonprincipal ideal of K remains nonprincipal in L.

Corollary 2 *Let ζ_p be a primitive* pth *root of unity, where p is a prime $\equiv$* 3 (mod 4). *Then every nonprincipal ideal of $\mathbf{Q}(\sqrt{-p})$ remains nonprincipal in the extension $\mathbf{Q}(\zeta_p)$.*

Proof In this case $K = \mathbf{Q}(\sqrt{-p})$, $F =$ the maximal real subfield of $\mathbf{Q}(\zeta_p)$, $L = \mathbf{Q}(\zeta_p)$. We observe that $[F : \mathbf{Q}] = (p-1)/2$ and $w = 2p$. Hence $(v, [F : \mathbf{Q}]) = 1$ and Theorem 1 is applicable. The result follows from the fact that K has odd class number.

Theorem 2 (Kitaoka [3]) *Let $\mathfrak{L}$, $\mathfrak{M}$ be definite binary quadratic lattices over $\mathbf{Z}$ and F a totally real extension of $\mathbf{Q}$. If Σ is an isometry of $\mathfrak{L} \otimes_{\mathbf{Z}} \mathcal{O}_F$ onto $\mathfrak{M} \otimes_{\mathbf{Z}} \mathcal{O}_F$, then $\Sigma(\mathfrak{L}) = \mathfrak{M}$.*

Proof The underlying quadratic number fields of $\mathfrak{L}$, $\mathfrak{M}$ are determined by their discriminants. If $\tilde{\mathfrak{L}}$, $\tilde{\mathfrak{M}}$ are isometric, then $\mathfrak{L}$, $\mathfrak{M}$ have the same discriminants. Hence we may assume that both are lattices in a single imaginary quadratic number field $K = \mathbf{Q}(\sqrt{-D})$. Furthermore, after scaling suitably, we may assume that the quadratic form on $\mathfrak{L}$ is the norm form n of K, while the quadratic form on $\mathfrak{M}$ is $c \cdot n$, c a positive rational number. Composing Σ with J, if necessary, we may take Σ to be proper. Then Σ is a proper similitude of norm c on the quadratic space (K, n). Any such proper similitude is multiplication by a nonzero element of L [1, p. 28]. Thus $\tilde{\mathfrak{M}} = \alpha\tilde{\mathfrak{L}}$ with $n(\alpha) = \alpha\alpha^J = c$. It suffices to show that $\alpha \in K$. From $\tilde{\mathfrak{M}} = \alpha\tilde{\mathfrak{L}}$ it follows that $\mathfrak{L}$, $\mathfrak{M}$ have the same order $\mathcal{O}$. We may as well assume that $\mathcal{O} \neq \mathcal{O}_K$ when $D = 1$ or 3. Furthermore, we may suppose that F is Galois over $\mathbf{Q}$. Imitating the proof of Lemma 1, we see that $\alpha^{1-\sigma} \in \tilde{\mathcal{O}} \cap U_L$ for all $\sigma \in G$. Thus $\alpha^{1-\sigma} \in U_F$ for all $\sigma \in G$, by Lemma 2. This implies $\alpha^{1-J} \in K$, which, in turn, implies $\alpha^2 \in K$. If $\alpha \in K$, we are done. If $\alpha \notin K$, then $K(\alpha)$ is a quadratic extension of K and, as a consequence of the Galois structure of L over $\mathbf{Q}$, $K(\alpha)$ is the compositum of K and a real quadratic field $\mathbf{Q}(\sqrt{r}) \subseteq F$. Thus we may as well assume $F = \mathbf{Q}(\sqrt{r})$, $L = K(\alpha)$. Let τ be the nontrivial element of G. Then $\alpha^\tau = -\alpha$. Suppose $\mathfrak{L} = \mathbf{Z}\lambda_1 + \mathbf{Z}\lambda_2$, $\mathfrak{M} = \mathbf{Z}\mu_1 + \mathbf{Z}\mu_2$.

Then $\mathfrak{M} = \alpha\tilde{\Omega}$ implies there exist $a_1, a_2, a_3, a_4 \in \mathcal{O}_F$ such that

$$a_1\mu_1 + a_2\mu_2 = \alpha\lambda_1, \qquad a_3\mu_1 + a_4\mu_2 = \alpha\lambda_2 \tag{3}$$

with $a_1 a_4 - a_2 a_3 \in U_F$. Applying τ to the equations (3) and adding, we obtain $a_i^\tau = -a_i$, $i = 1, 2, 3, 4$. Hence $a_i = b_i\sqrt{r}$ for some $b_i \in \mathbf{Z}$, $i = 1, 2, 3, 4$. Then $a_1 a_4 - a_2 a_3 = r(b_1 b_4 - b_2 b_3)$, which implies $r = 1$, a contradiction.

REFERENCES

[1] M. Eichler, "Quadratische Formen und orthogonale Gruppen." Springer-Verlag, Berlin–Göttingen–Heidelberg, 1952.
[2] H. Hasse, "Über die Klassenzahl abelscher Zahlkörper." Akademie-Verlag, Berlin, 1952.
[3] Y. Kitaoka, Scalar Extension of Quadratic Lattices (to appear).
[4] E. Weiss, "Algebraic Number Theory." McGraw-Hill, New York, 1963.

AMS (MOS) 1970 subject classifications: 10C05, 12A50.

Quartic Coverings of a Cubic†

BASIL GORDON *MURRAY SCHACHER*

UNIVERSITY OF CALIFORNIA
LOS ANGELES, CALIFORNIA

Any cubic extension of a number field is shown to be the resolvent cubic field of a generically irreducible quartic polynomial whose Galois group is the alternating group A_4. This is applied to the question of which groups can occur as Galois groups in finite-dimensional division algebras.

Introduction

Suppose $k \subset L$ are algebraic number fields. Following the terminology of Schacher [2] we shall say L is k-adequate if L is a maximal subfield of a finite-dimensional division algebra with center k. A finite group G will be called k-admissible if G is the Galois group of a normal extension L of k with L k-adequate.

In Schacher [2] it was asked whether the alternating group A_4 is Q-admissible, Q the field of rational numbers. We show in this note that in fact A_4 is k-admissible for all algebraic number fields k. This will follow from a general construction which realizes any cubic field as the resolvent cubic

† This work was supported under grant GP-33580, Basil Gordon, and GP-28696, Murray Schacher.

field of a covering quartic whose Galois group is A_4 and which satisfies prescribed local irreducibility conditions. We also study more closely the groups that are admissible over all number fields, with particular emphasis on the structure of their Sylow subgroups.

For notational purposes, a division ring D finite-dimensional and central over a field k will be called a k-division ring. Throughout this paper we use freely the theory of valuations or primes for algebraic number fields, and the theory of Hasse invariants of k-division rings. If k is a number field and q a prime of k, we write k_q for the completion of k at q. The order of a finite group G is denoted by $|G|$.

1. Groups Admissible over All Number Fields

It was proved in Schacher [2, 4.1] that all Q-admissible groups have metacyclic Sylow subgroups. The following theorem is of the same type, but with a stronger hypothesis and a stronger conclusion.

Theorem 1.1 *If a finite group G is k-admissible for all algebraic number fields k, then every Sylow subgroup of G is abelian and generated by two elements.*

Proof Suppose G satisfies the hypothesis of Theorem 1.1 and P is a Sylow subgroup of G, $|P| = p^a$, p a prime. We let $k = Q(\varepsilon_p a)$ where $\varepsilon_p a$ is a primitive p^ath root of unity. Since G is k-admissible, we have by [2, 2.6] G is the Galois group of a normal extension L of k, so that P is a subgroup of the local Galois groups $\mathrm{Gal}(L_{q_1}/k_{q_1})$ and $\mathrm{Gal}(L_{q_2}/k_{q_2})$ for some pair of primes q_1 and q_2 of k. Let M_i $(i = 1, 2)$ be the field corresponding to P in the Galois correspondence, so that $P = \mathrm{Gal}(Lq_i/M_i)$. The rational prime p has a unique totally ramified extension in k; thus one of the q_i, say q_1, does not lie over p. It follows that the extension Lq_1/M_1 is tamely ramified. Since ε_{p^a} is in M_1, we conclude by Albert [1, Theorem 4] that P is abelian. By [2, 4.1] P is either cyclic or the direct product of two cyclic groups. This completes the proof of Theorem 1.1.

It follows from Theorem 1.1 that the symmetric group S_4 is not admissible over all number fields. This answers a question raised in Schacher [2]. By Schacher [2, 2.8] S_3 is admissible over all number fields, and this shows that such groups need not be abelian or nilpotent. Of course A_4 satisfies the conclusion of Theorem 1.1; we shall show presently that it is admissible over all number fields. A_5 also satisfies the conclusion of Theorem 1.1; we do not know if it is admissible over all number fields. By Theorem 1.1 A_n is not

admissible over all number fields for $n \geq 6$ since its 2-Sylow subgroup is not abelian. We are not even aware of whether A_6 and A_7 are Q-admissible.

2. Covering a Resolvent Cubic

Suppose k is a number field and $h(z) = z^3 + az + b \in k[z]$ an irreducible cubic. Let $\theta_1, \theta_2, \theta_3$ be the roots of h. We set

$$f(x) = x^4 - (6y^2 + 2a)x^2 + 8(y^3 + ay + 6)x - (3y^4 + 6ay^2 + 12by - a^2) \tag{1}$$

where y is a parameter that will be specialized in k. It is easily verified that the resolvent cubic of $f(x)$ is

$$g(w) = w^3 + (6y^2 + 2a)w^2 + 4(3y^4 + 6ay^2 + 12by - a^2)w + (8y^6 + 40ay^4 + 160by^3 - 4a^2y^2 - 32aby - 8a^3 - 64b^2).$$

The roots of $g(w)$ are

$$w_i = 2a - 2y^2 + 4y\theta_i + 4\theta_i^2 \qquad (i = 1, 2, 3).$$

Thus $Q(w_i) = Q(\theta_i)$, $i = 1, 2, 3$. The discriminants of f and g are both equal to

$$2^{12}(y^3 + ay + 6)^2(-4a^3 - 27b^2), \tag{2}$$

while the discriminant of the field $Q(\theta_i)$ divides $-4a^3 - 27b^2$.

We specialize a bit further. Assume that a, b are algebraic integers and that $z^3 + az + b$ determines a cubic cyclic extension of k; thus its discriminant $-4a^3 - 27b^2$ is a square in k. This guarantees by (2) that the discriminant of $f(x)$ is a square in k, and so the Galois group of f is a subgroup of A_4. In fact $f(x)$ has Galois group A_4 if and only if it is irreducible. We aim for more; we shall show in fact that y can be chosen so that $f(x)$ is irreducible in $k_{q_1}[x]$ and $k_{q_2}[x]$ for two primes q_1 and q_2 of k. What follows is a description of how these primes are chosen.

Let q be a prime of k at which $z^3 + az + b$ is split completely; there are infinitely many such q available by the Tschebotarev density theorem. Then there is an algebraic integer $y_0 \in k$ so that $y_0^3 + ay_0 + b \equiv 0 \pmod{q}$. If $y_0^3 + ay_0 + b \not\equiv 0 \pmod{q^2}$, we stop at this point. Otherwise let π be an algebraic integer in k that is a uniformizing parameter at q. Then if $y_1 = y_0 + \pi$, we have

$$y_1^3 + ay_1 + b = y_0^3 + ay_0 + b + 3\pi^2 y_0 + \pi(3y_0^2 + a).$$

Thus $y_1^3 + ay_1 + b \not\equiv 0 \pmod{q^2}$ unless $q \mid 3y_0^2 + a$. But $3z^2 + a$ is the derivative of $h(z) = z^3 + az + b$, and these polynomials have no common roots (mod q) except for the finite set of primes q that divide the discriminant of h.

Let then q_1 and q_2 be primes for which $h(z)$ splits completely and which do not divide the discriminant of h. We also assume that $q_i \nmid 2$, $i = 1, 2$. By the Chinese remainder theorem and the discussion above we can choose an algebraic integer y of k so that

$$y^3 + ay + b \equiv 0 \pmod{q_i}$$

but

$$y^3 + ay + b \not\equiv 0 \pmod{q_i^2}, \qquad i = 1, 2.$$

We summarize this construction in:

Theorem 2.1 *Let k be an algebraic number field. Suppose the constants $a, b, y \in k$ and primes q_1, q_2 are determined as above. Then for $f(x)$ determined as in (1) we have:*

(a) *$f(x)$ is irreducible in $k_{q_1}[x]$ and $k_{q_2}[x]$.*
(b) *The Galois group of f over k is A_4.*

Proof If $f(x)$ is irreducible in $k_{q_1}[x]$, then it is irreducible in $k[x]$, so the order of the Galois group of f is divisible by 4. Since the resolvent cubic field of f is the field of the irreducible cubic $z^3 + az + b$, the order of this group is divisible by 3. But the Galois group of f is a subgroup of A_4 since the discriminant of f is a square, and so must be all of A_4. Thus (b) will follow from (a).

Let $q = q_1$ or q_2. Clearly f cannot be the product of a linear factor and an irreducible cubic in $k_q[x]$ since the resolvent cubic of f splits in $k_q[x]$. Thus if f is reducible over k_q, it must be a product of two quadratic factors (not necessarily irreducible themselves) in $k_q[x]$. In this event there are q-adic integers r, s, and t with

$$f(x) = (x^2 + rx + s)(x^2 - rx + t). \tag{3}$$

Identifying coefficients in (3) gives the equations

$$\begin{aligned} s + t - r^2 &= -(6y^2 + 2a) \\ r(t - s) &= 8(y^3 + ay + b) \\ st &= -(3y^4 + 6ay^2 + 12by - a^2). \end{aligned} \tag{4}$$

It is easily verified that $(3y^2 + a)^2 \equiv -(3y^4 + 6ay^2 + 12by - a^2) \pmod{q}$, and so $f(x) \equiv (x^2 - (3y^2 + a)^2)^2 \pmod{q}$. Thus in (4) we have

$$s \equiv t \equiv -(3y^2 + a) \pmod{q} \qquad \text{and} \qquad r \equiv 0 \pmod{q}.$$

Then $r(s - t) \equiv 0 \pmod{q^2}$, but $8(y^3 + ay + b) \not\equiv 0 \pmod{q^2}$ by construction. This contradiction establishes the irreducibility of $f(x)$ in $k_q[x]$.

We have the:

Corollary 2.2 *A_4 is admissible over all algebraic number fields.*

Proof Let k be a number field and $f(x)$ the quartic determined in Theorem 2.1. Let L be the splitting field of $f(x)$ over k. We wish to show L is k-adequate. By Schacher [2, 2.1] it is enough to show that the abelian group $H^2(A_4, L^*)$ has an element of order 12, where $L^* = L - \{0\}$. Since the 3-Sylow subgroup of A_4 is cyclic, $H^2(A_4, L^*)$ has an element of order 3 by Schacher [2, p. 455]. Thus it is enough to show that $H^2(A_4, L^*)$ has an element of order 4. Let D be the k-division ring with Hasse invariants determined by

$$\mathrm{inv}_{q_1}(D) = \tfrac{1}{4}, \qquad \mathrm{inv}_{q_2}(D) = -\tfrac{1}{4}, \qquad \mathrm{inv}_q(D) = 0, \quad q \neq q_1 \text{ or } q_2 .$$

Since $f(x)$ is irreducible at q_1 and q_2, $4 \mid [L_{q_i} : k_{q_i}]$ $(i = 1, 2)$ and so L splits D. This means that D determines an element of $H^2(A_4, L^*)$ of order 4, and L is k-adequate. But $\mathrm{Gal}(L/k) = A_4$, and so A_4 is k-admissible.

We close with an explicit example over the rational field Q. The irreducible cubic $Z^3 - 3Z - 1$ of discriminant 3^4 determines a cyclic cubic field over Q, so we choose $a = -3$, $b = -1$. If $y = 3$, then $y^3 + ay + b = 17$. Then the polynomial $f(x)$ becomes

$$f(x) = x^4 - 48x^2 + 136x - 36$$

with discriminant $2^{12}3^4 17^2$. An examination of the Newton polygon shows that f is irreducible in $Q_2[x]$, and the proof of Theorem 2.1 shows f irreducible in $Q_{17}[x]$. Let L be the root field of f over Q. Then $\mathrm{Gal}(L/Q) = A_4$ and L is Q-adequate.

We note that all of our remarks apply for global fields of characteristic not 2 or 3, and we get:

Corollary 2.3 *A_4 is k-admissible for all global fields k of characteristic $p \neq 2$ or 3.*

REFERENCES

[1] A. A. Albert, On p-adic fields and rational division algebras, *Ann. Math.* **41** (1940), 674–693.

[2] M. Schacher, Subfields of division rings I, *J. Algebra* **9** (1968), 451–477.

On Extremal Density Theorems for Linear Forms

R. L. GRAHAM *H. S. WITSENHAUSEN*

BELL LABORATORIES
MURRAY HILL, NEW JERSEY

J. H. SPENCER†

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CAMBRIDGE, MASSACHUSETTS‡

A typical question in extremal number theory is one which asks how large a subset R may be selected from a given set of integers so that R possesses some desired property. For example, it is not difficult to see that if R is a subset of the integers $[1, 2, \ldots, 2N]$ *and R has more than N elements then there are integers x and y in R so that* $x + y$ *is also in R. The sets* $\{1, 3, 5, \ldots, 2N - 1\}$ *or* $\{N + 1, N + 2, \ldots, 2N\}$ *show that this bound cannot be improved.*

In this note we prove several general results of this type. In particular, we show that if $R \subseteq \{1, 2, \ldots, N\}$ *and R has more than* $N - [N/n]$ *elements, then for some integers x and y, the integers* x, $x + y$, $x + 2y$, $\ldots$, $x + (n - 1)y$ *and y all belong to R. Furthermore the bound* $N - [N/n]$ *is best possible.*

† The work done by this author was done while he was a consultant at Bell Laboratories.
‡ Present address: SUNY at Stony Brook, Stony Brook, New York.

1. Introduction

Suppose $\mathscr{L} = \{L_i(x_1, \ldots, x_m) \equiv \sum_{j=1}^{m} a_{ij}x_j: 1 \leq i \leq n\}$ is a set of linear forms in the variables x_j with integer coefficients a_{ij}. The question we consider is the following:

How large may a subset R of $\{1, 2, \ldots, N\}$ be so that for every choice of positive integers t_j, $1 \leq j \leq m$, at least one of the values $L_i(t_1, \ldots, t_m)$, $1 \leq i \leq n$, is not in R.

Unfortunately, this question appears to be rather difficult and very few general results are currently available. In this paper we study this problem for several important special sets $\mathscr{L}$. It will be seen that even in these simple cases, the problem is not without interest.

2. Preliminaries

Let $[1, N]$ denote the set $\{1, 2, \ldots, N\}$. If $\mathscr{L} = \{L_i(x_1, \ldots, x_m): 1 \leq i \leq n\}$ is a set of linear forms, we say that a set $R \subseteq [1, N]$ is *$\mathscr{L}$-free* if for any choice of positive integers $t_1, \ldots, t_m$, at least one of the values $L_i(t_1, \ldots, t_m)$ does not belong to R. If R is not $\mathscr{L}$-free, we say that $\mathscr{L}$ *hits* R. Define

$$S_{\mathscr{L}}(N) = \max_{R} |R|$$

where the max is taken over all $R \subseteq [1, N]$ that are $\mathscr{L}$-free and $|R|$ denotes the cardinality of R. Also, define $\delta(\mathscr{L})$, called the *critical density* of $\mathscr{L}$, by

$$\delta(\mathscr{L}) = \liminf_{N} S_{\mathscr{L}}(N)/N.$$

As an example, consider the system $\mathscr{L}_n = \{x_1 + kx_2: 0 \leq k < n\}$. The condition that R is $\mathscr{L}_n$-free means exactly that R contains no arithmetic progression of n terms.

For this example, a recent result of Szemerédi [2], however, asserts that any infinite set of integers of positive upper density contains arbitrarily long arithmetic progressions. From this it follows at once that $\delta(\mathscr{L}_n) = 0$.

3. Augmented Arithmetic Progressions

We now consider a system closely related to $\mathscr{L}_n$ which we denote by $\mathscr{L}_n^*$. It is defined by

$$\mathscr{L}_n^* = \{x_1 + kx_2: 0 \leq k < n\} \cup \{x_2\}.$$

In this case, $\mathscr{L}_n^*$ hits R if and only if R contains an arithmetic progression of

n terms together with the common difference of the progression. However, the critical density of $\mathscr{L}_n^*$ differs sharply from that of $\mathscr{L}_n$ as the following examples indicate.

Example 1 Let $R_1 \subseteq [1, N]$ be defined by

$$R_1 = \{x \in [1, N]: x > [N/n]\}.$$

Clearly R_1 is $\mathscr{L}_n^*$-free since

$$t_1 + (n-1)t_2 \geq n(1 + [N/n]) > N \qquad \text{for} \quad t_1, t_2 \in R_1.$$

Thus

$$\delta(\mathscr{L}_n^*) \geq 1 - n^{-1}. \tag{1}$$

Example 2 Suppose n is prime and let $R_2 \subseteq [1, N]$ be defined by

$$R_2 = \{x \in [1, N]: x \not\equiv 0 \pmod{n}\}.$$

Then $\mathscr{L}_n^*$ cannot hit R_2 since for *any* integers t_1 and t_2, either $t_2 \equiv 0 \pmod{n}$ or $t_1 + kt_2$, $0 \leq k < n$, runs through a complete residue system modulo n and therefore represents $0 \notin R_2$. Note that

$$|R_2| = N - [N/n] = |R_1|. \tag{2}$$

The following result shows that equality holds in (1) and, in fact, (2) is best possible.

Theorem 1 *Suppose* $R \subseteq [1, N]$ *with* $|R| > N - [N/n]$. *Then* $\mathscr{L}_n^*$ *hits* R.

Proof Let R satisfy the hypothesis of the theorem and suppose R is $\mathscr{L}_n^*$-free. Let Δ denote the least element of R. Then we may assume

$$\Delta \leq [N/n] \tag{3}$$

since otherwise $|R| \leq N - [N/n]$. Define the arithmetic progressions $T_i \subseteq [1, N]$ by

$$T_i = \{i + k\Delta: 0 \leq k < n\}, \qquad 1 \leq i \leq N - (n-1)\Delta.$$

Also, define A_j, $A_j' \subseteq [1, N]$ for $1 \leq j \leq n$ as follows:

$$A_j = \begin{cases} [(j-1)\Delta + 1, j\Delta] & \text{for} \quad 1 \leq j < n, \\ [(n-1)\Delta + 1, N] & \text{for} \quad j = n; \end{cases}$$

$$A_j' = \begin{cases} [N - j\Delta + 1, N - (j-1)\Delta] & \text{for} \quad 1 \leq j < n, \\ [1, N - (n-1)\Delta] & \text{for} \quad j = n. \end{cases}$$

By (3), we see that

$$|A_n| = |A_n'| \geq \Delta.$$

Also, it is easily checked that if $x \in A_j \cap A'_{j'}$ then $j + j' = n + t$ for some t, $1 \le t \le n$, and

$$|\{i: x \in T_i\}| = t. \tag{4}$$

We claim the following equation holds:

$$n|R| = \sum_{i=1}^{N-(n-1)\Delta} |T_i \cap R| + \sum_{j=1}^{n-1} (n-j)(|A_j \cap R| + |A'_j \cap R|). \tag{5}$$

To prove (5), let $x \in R$. Then for some k and k', $x \in A_k \cap A'_{k'}$. Since the A_j are disjoint, as are the A'_j, then the contribution x makes to the second sum on the right-hand side of (4) is just $(n-k) + (n-k')$. Let $k + k' = n + t$. Hence, by (4), x contributes exactly t to the first sum in (5). Therefore, each $x \in R$ contributes exactly

$$(n-k) + (n-k') + (k + k' - n) = n$$

to the right-hand side of (5) so that Eq. (5) is indeed valid. But by hypothesis, since $\Delta \in R$, then $|T_i \cap R| \le n-1$ for all i. Thus, since $|A_1 \cap R| = 1$, then by (5)

$$\begin{aligned} n|R| &\le (n-1)(N-(n-1)\Delta) + 2\Delta \sum_{j=1}^{n-1} (n-j) - (n-1)(\Delta - 1) \\ &= (n-1)N + \Delta(-(n-1)^2 + n(n-1) - (n-1)) + n - 1 \\ &= (n-1)(N+1), \end{aligned} \tag{6}$$

which implies

$$|R| \le \left\lfloor \frac{(n-1)(N+1)}{n} \right\rfloor = N - \left\lceil \frac{N}{n} \right\rceil. \tag{7}$$

This proves Theorem 1. ∎

Of course, it follows from (1) and (7) that

$$S_{\mathscr{L}_n^*}(N) = N - [N/n] \tag{8}$$

and consequently

$$\delta(\mathscr{L}_n^*) = 1 - n^{-1}.$$

4. Forms in One Variable—A Special Case

As a prelude to a discussion in the next section of the general case of linear forms in one variable (i.e., with $m = 1$), we consider first the special

case $\mathscr{L} = \{x, 2x, 3x\}$. This example in fact has all the essential features of the general case.

To begin, we let $D = \{d_1 < d_2 < \cdots\}$ denote the set of all integers of the form $2^a 3^b$, $a, b \geq 0$.

Let N be a fixed positive integer. For $1 \leq t \leq N$ with $(t, 6) = 1$, let $C(t)$ denote the set

$$C(t) = [1, N] \cap \{td_k : k = 1, 2, \ldots\}.$$

Note that a set $R \subseteq [1, N]$ is $\mathscr{L}$-free if and only if $R(t) = R \cap C(t)$ is $\mathscr{L}$-free for all t with $(t, 6) = 1$. For indeed, $\mathscr{L}$ can hit R only if for some x, $\{x, 2x, 3x\} \supseteq R$. However, this implies that $\mathscr{L}$ hits $R(t)$ for some t relatively prime to 6. Thus, a maximal $\mathscr{L}$-free set R is formed by taking the union of maximal $\mathscr{L}$-free subsets from $C(t)$ for each t, $(t, 6) = 1$. However, it is clear that

$$X_t = \{td_k : k = 1, \ldots, r\} \subseteq C(t)$$

is $\mathscr{L}$-free if and only if $X_1 = \{d_k : k = 1, \ldots, r\} \subseteq C(1)$ is $\mathscr{L}$-free. Thus, if $f(r)$ denotes the cardinality of the largest $\mathscr{L}$-free subset of $\{d_1, \ldots, d_r\}$ and $h(r)$ denotes the number of $t \in [1, N]$, $(t, 6) = 1$, with $|C(t)| = r$, then for any $\mathscr{L}$-free set $R \subseteq [1, N]$,

$$|R| \leq \sum_{r=1}^{\infty} f(r)h(r). \tag{9}$$

For fixed r, $|C(t)| = r$ if and only if

$$td_r \leq N < td_{r+1}$$

i.e.,

$$N/d_{r+1} < t \leq N/d_r .$$

Thus,

$$h(r) \to \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)N\left(\frac{1}{d_r} - \frac{1}{d_{r+1}}\right) \quad \text{as} \quad N \to \infty \tag{10}$$

and, therefore, for maximal $\mathscr{L}$-free sets $R_N \subseteq [1, N]$,

$$\lim_{N\to\infty} \frac{|R_N|}{N} = \frac{1}{3} \sum_{r=1}^{\infty} f(r)\left(\frac{1}{d_r} - \frac{1}{d_{r+1}}\right). \tag{11}$$

But

$$f(r + 1) - f(r) \leq 1,$$

so that letting $K(\mathscr{L})$ denote the set $\{k: f(k) > f(k-1)\}$, the telescoping sum in (11) becomes

$$\delta(\mathscr{L}) = \frac{1}{3} \sum_{k \in K(\mathscr{L})} \frac{1}{d_k}. \tag{12}$$

Unfortunately, there does not seem to be any simple way to determine the elements of $K(\mathscr{L})$. The first few values are given in Table 1.

TABLE 1

k	$f(k)$	k	$f(k)$	k	$f(k)$
1	1	13	9	25	17
2	2	14	10	26	18
3	2	15	11	27	18
4	3	16	11	28	19
5	4	17	12	29	20
6	5	18	13	30	20
7	5	19	13	31	21
8	6	20	14	32	22
9	7	21	14	33	22
10	7	22	15	34	23
11	8	23	16	35	24
12	8	24	17	36	25

Thus,

$$K(\mathscr{L}) = \{1, 2, 4, 5, 6, 8, 9, 11, 13, 14, 15, 17, 18, 20,$$
$$22, 23, 24, 26, 28, 29, 31, 32, 34, 35, 36, \ldots\}. \tag{13}$$

It may be that $f(k) = 1 + [2k/3]$ if $k \not\equiv 0 \pmod 3$ and, perhaps, for all k, there is always a maximal $\mathscr{L}$-free set

$$R_k = \{2^{a_i}3^{b_i}: i = 1, \ldots, f(k)\} \subseteq \{d_1, \ldots, d_k\}$$

in which all $a_i - b_i$ are congruent modulo 3.

It would also be interesting to know if $\delta(\mathscr{L})$ is irrational.

5. Forms in One Variable—The General Case

Let $\mathscr{L}$ denote the set of linear forms $\{a_1 x, \ldots, a_n x\}$ where $A = \{a_1 < \cdots < a_n\}$. Let $P(A) = \{q_1, \ldots, q_r\}$ be the set of primes dividing the a_i and let $D^{(\mathscr{L})} = (d_1 < d_2 < \cdots)$ denote the set of all integers of the form

$q_1^{\alpha_1} \cdots q_r^{\alpha_r}$, $\alpha_i \geq 0$. For each k let $f(k)$ denote the cardinality of a maximal $\mathscr{L}$-free subset of $\{d_1, \ldots, d_k\}$. Finally, let $K(\mathscr{L})$ be defined by

$$K(\mathscr{L}) = \{k : f(k) > f(k-1)\}.$$

By using essentially the same arguments as in the previous section, the following theorem can be proved.

Theorem 2

$$\delta(\mathscr{L}) = \prod_{j=1}^{r} (1 - q_j^{-1}) \sum_{k \in K(\mathscr{L})} d_k^{-1} \tag{14}$$

6. Concluding Remarks

One problem with a representation such as (14) is that it is not clear how to describe $K(\mathscr{L})$ so as to be able to evaluate $\sum_{k \in K(\mathscr{L})} d_k^{-1}$. Several systems $\mathscr{L} = \mathscr{L}(a_1, \ldots, a_n) = \{a_1 x, \ldots, a_n x\}$ of forms in one variable are known, however, for which such a description can be given. We list a sample of these below. The arguments needed to determine the sets $K(\mathscr{L})$ are not difficult and are omitted.

1. $\delta(\mathscr{L}(1, p, p^2, \ldots, p^{m-1})) = (p^m - p)/(p^m - 1)$ for p prime. Thus, $\delta(\mathscr{L}(1, 2)) = \frac{2}{3}$ as expected.
2. $\delta(\mathscr{L}(1, n)) = n/(n+1)$.
3. $\delta(\mathscr{L}(2, 3)) = \frac{3}{4}$.
4. $\delta(\mathscr{L}(1, 2, 8)) = \frac{57}{62}$. Some recent results of Harlambis [1] are relevant here.

It seems quite likely that almost all systems $\mathscr{L}$ have $\delta(\mathscr{L})$ irrational although not even *one* such $\mathscr{L}$ is known at present!

REFERENCES

[1] N. M. Harlambis, "Sets with missing differences or missing patterns," PhD Dissertation, Univ. California, Los Angeles, 1973.

[2] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.* **27** (1975), 199–245.

Aliquot Sequences

RICHARD K. GUY

UNIVERSITY OF CALGARY
CALGARY, ALBERTA, CANADA

...m'a fait songer au théorème empirique *suivant:*

n étant un nombre entier, soit n_1 *la somme des diviseurs de n, inférieurs à n, soit* n_2 *la somme des diviseurs de* n_1, *inférieurs à* n_1 *; etc. Cela posé: les nombres* $n, n_1, n_2, \ldots$ *tendent vers une limite* λ, *laquelle est* 1 *ou un nombre parfait.*

E. CATALAN [5]

This is the origin of the Catalan–Dickson conjecture. Dickson [9] pointed out that the sequence will sometimes cycle between the members of an amicable pair, or round some larger cycle, though at the time no such cycle was known.

La période peut avoir plus de deux termes, qu'on pourrait appeler, pour garder la même terminologie, des nombres sociables. *Par exemple le nombre* 12496 *engendre une période de* 4[sic] *termes, le nombre* 14316 *une période de* 28 *termes.*

Enfin dans certain cas, on arrive à des nombres très grands qui rendent le calcul insupportable. Exemple: le nombre 138.

P. POULET [21]

Poulet's calculations led him to believe the contrary of the Catalan–Dickson conjecture, namely that there are sequences that increase

indefinitely, albeit somewhat erratically. Selfridge and the present writer, with considerable computational help from others [1, 2, 8, 11, 16, 17, 19, 20] have offered both experimental and heuristic evidence [13–15, 23] for the almost diametrically opposite conjecture that almost all even aliquot sequences are unbounded.

Let $s(n)$ be the sum of the **aliquot parts** of n (divisors of n other than n itself so that $s(n) = \sigma(n) - n$, where $\sigma(n)$ is the usual sum of divisors function. Define $s^0(n) = n$, and, for $k \geqslant 1$,

$$s^k(n) = s(s^{k-1}(n)),$$

(here often written $n : k$). D. H. Lehmer answered Poulet's question about 138 by showing that the sequence has a maximum

$$179931\ 895322 = 138 : 117 = 2 \cdot 61 \cdot 929 \cdot 1587569,$$

and that $138 : 177 = 1$. The next number to give difficulty is 276. Computations were made by Paxson [19, 20], by Cohen [6], and, much more extensively, by Lehmer, and our present state of knowledge of the 276 sequence is

$$107100\ 047962\ 427456\ 048833\ 497403\ 019424 = 276 : 433 = 2^5 3 \cdot 199 \cdot c,$$

where c is a 31-digit composite number with no small factors. The desire to calculate such sequences has been one of a number of stimuli leading to the development of a variety of new algorithms for factoring large numbers [12].

Another question asked by Poulet concerned the existence of cycles of periods other than 1, 2, 5, and 28. In particular it is still not known if period 3 can occur. Comparatively recently 14 cycles of period 4 have been found by Borho [4], Cohen [6], David [7] and Root [3], namely those for

$n = 1264460,\ 2115324,\ 2784580,\ 4938136,\ 7169104,$

$18048976,\ 18656380,\ 28158165,\ 46722700,\ 81128632,$

$174277820,\ 209524210,\ 330003580,\ 498215416.$

An interesting example of a periodic sequence is 17490, for which $17490 : 228 = 1264460$, the smallest member of the smallest of these 4-cycles.

So aliquot sequences may be classified as **terminating** if a value of k is known such that $n : k = 1$, or **periodic** if numbers $c \geqslant 1$ and k are known such that $n : k = n : c + k$, or **incomplete** otherwise. Since knowledge is steadily advancing, membership of these classes varies with time. A good deal of calculation has been done at levels greater than 10^{24}: For example, the Lehmers have investigated the following sequences, in addition to that for 276:

$$35149\ 477396\ 986268\ 016618\ 686344\ 127020 = 552 : 181 = 2^2 3^2 5 \cdot 7^2 c,$$

$$2\ 422499\ 075303\ 417661\ 059252\ 663526 = 564 : 265 = 2 \cdot 3^2 23 \cdot 89 \cdot c,$$

$$166\,036689\,342670\,728789\,598390\,618080 = 660 : 168$$
$$= 2^5 3 \cdot 5 \cdot 7 \cdot 11 \cdot 37 \cdot c,$$
$$8\,636062\,816231\,780695\,927699\,123810 = 840 : 195$$
$$= 2 \cdot 3^2 5 \cdot 7 \cdot 53 \cdot c,$$
$$34\,177685\,625161\,284824\,431442\,117328 = 966 : 184$$
$$= 2^4 7^3 139 \cdot c;$$

H. J. Godwin (written communication) has calculated

$$8502\,332502\,428553\,163137\,122717\,455339\,104096 = 1074 : 849$$
$$= 2^5 3 \cdot 31 \cdot 457 \cdot c,$$

(assuming that a 38-digit pseudoprime in term 847 is prime) and

$$60012\,099828\,734883\,991294\,272626\,672754 = 1464 : 530 = 2 \cdot 3 \cdot 29 \cdot x,$$

where x was still to be tested; and Selfridge and Wunderlich (see [14, 17]) have pursued all sequences starting below 10^4 to beyond 10^{24}. However, only one sequence, 4488, has exceeded this level:

$$1\,807814\,653481\,873196\,164108 = 4488 : 459$$
$$= 2^2 13 \cdot 991 \cdot 146819 \cdot 3201581 \cdot 74632871,$$

and later been found to terminate, $4488 : 801 = 1$.

Devitt [8] has pursued all even numbers in the ranges $(10^k + 2, 10^k + 100)$ $k = 9$, 10, 11 and 12 (see also [16]) and found the following numbers of the three classes of sequences:

$k =$	9	10	11	12
terminating	161	146	139	113
periodic	7	4	4	4
incomplete at 10^{18}	332	350	357	383.

The steady increase of the numbers of incomplete sequences is, of course, partly accounted for by the fact that the later samples start somewhat nearer the arbitrary bound, 10^{18}, but this effect is only marginal, and if we calculate the *average order* of $s(n)$ for n even (e.g., by the method given in Hardy and Wright [18, Theorem 324] we obtain

$$n(5\pi^2/24 - 1) \approx 1.05617n > n,$$

so that, on average, such sequences can be expected to increase. In [15] Selfridge and the present writer give detailed consideration to the various

guides and *drivers* (see below) which control aliquot sequences. Similar ideas are outlined by Wunderlich [23], and by Devitt [8, Chapter 4].

H. J. J. te Riele [22] has constructed an aliquot sequence containing 5092 (and almost certainly many more) monotonically increasing terms. A most interesting remark in te Riele's paper is the last sentence stating that H. W. Lenstra can prove the existence of *arbitrarily long* monotonically increasing aliquot sequences. Versions of Lenstra's proof are given by Erdős [10] and Devitt [8, pp. 42–44]. Erdős also proves the stronger result:

Theorem *For all n except a sequence of density 0, and for every k and $\delta > 0$,*

$$(1-\delta)n\left(\frac{s(n)}{n}\right)^i < s^i(n) < (1+\delta)n\left(\frac{s(n)}{n}\right)^i$$

for $1 \leqslant i \leqslant k$.

Here we use Lenstra's method to establish the following remarkable result:

Theorem *Given any prime p_k, any integer t, and any real number $\rho > 1$, there are aliquot sequences containing t consecutive terms, each greater than ρ times the previous one, but whose only prime divisors exceed p_k.*

Proof We construct such a sequence,

$$n = n:0, \quad n:1, \quad n:2, \quad \ldots, \quad n:t,$$

where, for $0 \leqslant r \leqslant t$,

$$n:r = p_{k+1}^{a_1} p_{k+2}^{a_2} \cdots p_{k+l}^{a_l} \cdots p_{k+l+t-r}^{a_{l+t-r}} m_r,$$

and none of the first $k + l + t - r$ primes divide m_r.

First choose l so that the sequence diverges with the required rapidity. For $0 \leqslant r \leqslant t-1$,

$$\begin{aligned}
\frac{n:r+1}{n:r} = \frac{s(n:r)}{n:r} &= \frac{\sigma(n:r)}{n:r} - 1 \\
&= \frac{\sigma(p_{k+1}^{a_1} p_{k+2}^{a_2} \cdots p_{k+l+t-r}^{a_{l+t-r}} m_r)}{p_{k+1}^{a_1} p_{k+2}^{a_2} \cdots p_{k+l+t-r}^{a_{l+t-r}} m_r} - 1 \\
&= \frac{\sigma(p_{k+1}^{a_1})}{p_{k+1}^{a_1}} \cdot \frac{\sigma(p_{k+2}^{a_2})}{p_{k+2}^{a_2}} \cdots \frac{\sigma(m_r)}{m_r} - 1 \\
&> \frac{\sigma(p_{k+1}^{a_1})}{p_{k+1}^{a_1}} \frac{\sigma(p_{k+2}^{a_2})}{p_{k+2}^{a_2}} \cdots \frac{\sigma(p_{k+l}^{a_l})}{p_{k+l}^{a_l}} - 1 \\
&> \frac{p_{k+1}+1}{p_{k+1}} \cdot \frac{p_{k+2}+1}{p_{k+2}} \cdot \cdots \cdot \frac{p_{k+l}+1}{p_{k+l}} - 1,
\end{aligned}$$

and since $\prod (1 + p^{-1})$ diverges, we may choose l (e.g., $l = \lfloor k^{\rho+1} \rfloor$) to make the ratio greater than ρ.

Next choose a_1 to exclude the first k primes as factors of the $n:r$, e.g., $a_1 = \phi(p_1^2 p_2^2 \cdots p_k^2) - 1$. By the Euler–Fermat theorem, since $(p_i, p_{k+1}) = 1$ for $1 \leqslant i \leqslant k$,

$$p_{k+1}^{p_i - 1} \equiv 1 \bmod p_i ,$$

so $p_{k+1}^{a_1+1} \equiv 1 \bmod p_i$, and $p_i | \sigma(p_{k+1}^{a_1})$, $p_i | \sigma(n:r)$, and since $p_i \nmid n:r$, $p_i \nmid s(n:r) = n:r+1$ for $0 \leqslant r \leqslant t-1$ and each i, $1 \leqslant i \leqslant k$.

Finally, choose the remaining a_{j+1}, $1 \leqslant j \leqslant l + t - 1$, recursively, so as to ensure that

$$p_{k+j}^{a_j} \parallel n:r \qquad \text{for} \quad 1 \leqslant j \leqslant l + t - r.$$

E.g., take $a_{j+1} = \sigma(p_{k+j}^{a_j+1}) - 1$, so that, as before,

$$p_{k+j+1}^{a_{j+1}+1} \equiv 1 \bmod p_{k+j}^{a_j+1},$$

so $p_{k+j}^{a_j+1} | \sigma(p_{k+j+1}^{a_{j+1}})$, $p_{k+j}^{a_j+1} | \sigma(n:r)$, and since $p_{k+j}^{a_j} \parallel n:r$, we have

$$p_{k+j}^{a_j} \parallel s(n:r) = n:r+1, \qquad 0 \leqslant r \leqslant t-1. \quad \blacksquare$$

As can be seen from the form of the proof, the powers of the primes used are subject to eventual erosion. Dickson [9] looked for combinations of powers of small primes that would "lock in," but any such search is doomed to failure; in fact Selfridge and the present author [15] give the following result.

Theorem *For any d, there is some prime divisor of d that does not divide $\sigma(d)/d$.*

On the other hand, some combinations do have remarkably long "lives," and these are important in making quantitative estimates. We restrict our attention to the factors of $\sigma(2^a) = 2^{a+1} - 1$. Define a **guide** g to be $g = 2^a v$ where v divides $\sigma(2^a)$. If also 2^{a-1} divides $\sigma(v)$, the guide is called a **driver**. If $g = 2^a v$ divides n and $2^a \parallel n$, g is said to be a **guide of (driver of)** n. Drivers include the even perfect numbers; there are only finitely many others.

Theorem [15] *The only drivers are* 2, $2^2 3$, $2^3 3 \cdot 5$, $2^5 3 \cdot 7$, $2^9 3 \cdot 11 \cdot 31$ *and the even perfect numbers.*

We may calculate the average order of $s(n)/n$ for those n having a given guide, and this gives an estimate of the **amplification** of that guide, or expected ratio of $s(n)/n$ while the guide is in control of the sequence. Table 1 [8, p. 58] gives calculated amplifications for some of the more commonly occurring guides, and compares them with the results obtained from studying more than 186,000 terms, lying between 10^5 and 10^{18}, of the 2000 sequences

with n even, $10^k + 2 \leqslant n \leqslant 10^k + 1000$, $9 \leqslant k \leqslant 12$. Less than 15000 terms had guides with powers of 2 greater than the fourth, or odd guides.

TABLE 1

Guide	Number of occurrences	Calculated amplification	Observed amplification
2	46526	$\pi^2/6 - 1 = 0.64493$	0.62787
$2 \cdot 3$	24323	$\pi^2/4 - 1 = 1.46740$	1.26744
2^2	32573	$3\pi^2/14 - 1 = 1.11492$	1.07573
2^27	27607	$\pi^2/4 - 1 = 1.46740$	1.40354
2^3	10014	$\pi^2/5 - 1 = 0.97392$	0.97143
2^33	6018	$3\pi^2/10 - 1 = 1.96088$	1.69723
2^35	5097	$5\pi^2/18 - 1 = 1.74156$	1.38542
$2^33 \cdot 5$	2917	$\pi^2/3 - 1 = 2.28987$	2.17929
2^4	11708	$15\pi^2/62 - 1 = 1.38781$	1.34447
2^431	4919	$\pi^2/4 - 1 = 1.46740$	1.44918

The agreement between theory and practice is as good as one can expect. "Typical" behavior cannot be expected unless the number of prime factors is "large"; that is, when $\ln \ln n$ is large, which is when n is well beyond computer range. The only even guides with amplification less than 1 are 2 and (but only just!) 2^3. These two account for 56 540 of the terms examined, less than one-third of the total.

One can also estimate, and observe, the **break probability** for a guide to change to a different guide, and the **life** of a guide, or expected number of terms in a sequence before the guide changes.

For example, the break probabilities for the 2-driver and for the 2^3 guide, among terms of size n are approximately

$$\tfrac{3}{2} \ln n \qquad \text{and} \qquad (\ln \ln n)^2/3 \ln n,$$

and the corresponding lives are approximately

$$5(\ln n)/9 \qquad \text{and} \qquad 3(\ln n)/(\ln \ln n)^2.$$

With the previously calculated amplifications, we can estimate the size of a term after an average run under the control of a given guide. For these two guides we can expect a term of size n to become of the order

$$n^{3/4} \qquad \text{and} \qquad n^{1-(\ln \ln n)^2/14}.$$

For the sample of 2000 sequences mentioned above, the observed lives were

$$9.33 \qquad \text{and} \qquad 2.7.$$

The fact that these are less than the estimates is again due to the fact that the size of term that can be investigated by computer is far too small to exhibit typical behavior.

The general behavior of aliquot sequences may be considered as a Markov process whose states are determined by the guides that are in control. The limit of the powers of the stochastic matrix associated with the same 2000 sequences yields the following probabilities of the seven most popular guides being in control:

2	2.3	2^2	2^27	2^3	2^4	2^431
0.2256	0.1025	0.1535	0.1851	0.0482	0.0580	0.0481,

accounting for 0.821 of the total probability. If we use these (and the other) probabilities to make a weighted average of the amplifications we obtain the figure

$$1.05745,$$

in very good agreement with the calculated amplification, mentioned before, the average order of $s(n)/n$ taken over all even numbers,

$$5\pi^2/24 - 1 \approx 1.05617.$$

It is highly unlikely that the Catalan–Dickson conjecture can be refuted, but the circumstantial evidence against it seems to have become overwhelming.

REFERENCES

[1] Jack Alanen, "Empirical Study of Aliquot Series." Math. Rep. No. 133, Stichting Math. Centrum, Amsterdam, July, 1972; reviewed in *Math. Comput.* **28** (1974), 878–879.

[2] Jack Alanen, "Tables of Aliquot Sequences," seven vols. of computer output, lodged with R. K. Guy, Univ. of Calgary; reviewed in *Math. Comput.* **28** (1974), 879–880.

[3] M. Beeler, R. W. Gosper, and R. Schroeppel, M.I.T. Artificial Intelligence Memo 239, 72-02-29.

[4] W. Borho, Über die Fixpunkte der k-fach iterierten Teilersummenfunktion, *Mitt. Math. Gesellsch. Hamburg* **4** (1969), 35–38; *MR* **40**, No. 7189.

[5] E. Catalan, *Bull. Soc. Math. France* **16** (1887–88), 128–129.

[6] H. Cohen, On amicable and sociable numbers, *Math. Comput.* **24** (1970), 423–429; *MR* **42**, No. 5887.

[7] Richard David, letter to D. H. Lehmer, 72-02-25.

[8] J. S. Devitt, Aliquot sequences, M.Sc. thesis, Univ. of Calgary, May 1976.

[9] L. E. Dickson, Theorems and tables on the sum of the divisors of a number, *Quart. J. Math.* **44** (1913), 264–296.

[10] Paul Erdős, On asymptotic properties of aliquot sequences, *Math. Comput.* **30** (1976), 641–645.

[11] J. Gillogly, Table of aliquot sequences 10^6 to $10^6 + 10^5$ (unpublished).

[12] Richard K. Guy, How to factor a number. Congressus Numerantium XVI, Proc. 5th Manitoba Conf. Numerical Math., Winnipeg, 1975, 49–89.

[13] Richard K. Guy and J. L. Selfridge, Interim report on aliquot series. Congressus Numerantium V. Proc. Manitoba Conf. Numerical Math., Winnipeg, 1971, 557–580; *MR* **49**, No. 194.

[14] Richard K. Guy and J. L. Selfridge, Combined report on aliquot sequences, Univ. of Calgary Math. Res. Paper 225, May 1974.

[15] Richard K. Guy and J. L. Selfridge, What drives an aliquot sequence?, *Math. Comput.* **29** (1975), 101–107.

[16] Richard K. Guy and M. R. Williams, Aliquot sequences near 10^{12}. Congressus Numerantium XII. Proc. 4th Manitoba Conf. Numerical Math., Winnipeg, 1974, 387–406.

[17] Richard K. Guy, D. H. Lehmer, J. L. Selfridge, and M. C. Wunderlich, Second report on aliquot sequences. Congressus Numerantium IX. Proc. 3rd Manitoba Conf. Numerical Math., Winnipeg, 1973, 357–368; *MR* **50**, No. 4455.

[18] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, 4th ed. Oxford Univ. Press, London and New York, 1968.

[19] G. Aaron Paxson, Aliquot sequences (preliminary report). *Amer. Math. Monthly* **63** (1956), 614.

[20] G. Aaron Paxson, Table of aliquot sequences. Deposited in UMT file 1966, reviewed in *Math. Comput.* **26** (1972), 807–809.

[21] P. Poulet, Question 4865, *L'Intermèdiaire des math.* **25** (1918), 100–101.

[22] H. J. J. te Riele, A note on the Catalan–Dickson conjecture, *Math. Comput.* **27** (1973), 189–192; *MR* **48**, No. 3869.

[23] M. C. Wunderlich, The Guy–Selfridge case against the Catalan–Dickson conjecture (mimeographed lecture notes).

AMS (MOS) 1970 subject classification: 10A20.

Integral Matrices A for which $AA^T = mI$

MARSHALL HALL, JR.†

CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CALIFORNIA

1. Introduction

An arithmetical problem of some interest is the study of integral matrices A for which AA^T is of some special form. The incidence matrix A of a symmetric block design with parameters v, k, λ is a (0, 1) matrix of order v satisfying $AA^T = (k - \lambda)I + \lambda J = B$, J being the matrix of order v all of whose entries are 1. The case we are interested in here is that of an integral matrix A of order n such that $AA^T = mI$. This includes all permutation matrices when $m = 1$, and the Hadamard matrices $H = [h_{ij}]$ of order n for which every $h_{ij} = \pm 1$ and $HH^T = nI_n$.

It is easy to find necessary and sufficient conditions that $AA^T = mI_n$ have an integral solution A of order n. These are: (1) if n is odd, m is a square; (2) if $n \equiv 2 \pmod 4$, $m = a^2 + b^2$; (3) if $n \equiv 0 \pmod 4$, m is any positive integer. These conditions are established in Section 2, and are necessary for the existence of a rational A and sufficient for the existence of an integral A.

If X is the r by n integral matrix consisting of the first r rows of an A for

† This research was supported in part by NSF Grant MPS 72-05035 A02.

which $AA^T = mI$, then necessarily $XX^T = mI_r$. The difficult and challenging problem is that in which we are given an r by n matrix X with $XX^T = mI_r$ to find whether or not there is an A with $AA^T = mI$ that has X as its first rows. This we call the completion problem. In Section 3 using results of [2], we can show that there is always a rational completion (m and n satisfying the preceding conditions), that is an A with X as its first rows and its remaining rows rational.

In Section 4 it is shown that if there are only one or two rows to be added to X, then there is an integral completion A. In Section 5 the case of Hadamard matrices is examined more carefully and it is shown that if at most four rows need to be added to an X there is a Hadamard completion. But there are Hadamard X's that do not have Hadamard completions, though they may have integral completions, as an example shows.

2. Existence Conditions

Following the methods of Chowla–Ryser [1] we can easily determine exactly conditions for the existence of an integral square matrix A of order n such that $A^TA = mI$.

Theorem 2.1 *There exists an integral square matrix A of order n such that $A^TA = mI$, m a positive integer if and only if:*

(i) *for n odd m is a square, $m = m_1^2$;*
(ii) *for $n \equiv 2 \pmod 4$ m is a sum of two integral squares, $m = a^2 + b^2$;*
(iii) *for $n \equiv 0 \pmod 4$ m is any positive integer.*

Proof Let $A = [a_{ij}]$, $i, j = 1, \ldots, n$. Let $x_1, \ldots, x_n$ be indeterminates. Let us write

$$L_i = \sum_j a_{ij}x_j, \qquad i = 1, \ldots, n. \tag{2.1}$$

Then the matrix equation

$$A^TA = mI \tag{2.2}$$

is equivalent to the identity

$$L_1^2 + \cdots + L_n^2 = m(x_1^2 + \cdots + x_n^2), \tag{2.3}$$

as is well known from the theory of quadratic forms, but a direct check is easy in this case.

Taking determinants of both sides of (2.2) we have

$$(\det A)^2 = m^n \tag{2.4}$$

from which it readily follows that if n is odd, then m must be a square $m = m_1^2$, then taking $A = m_1 I$, Eq. (2.2) is satisfied.

From here on let us suppose that n is even. Then from the theorem of Lagrange† any positive integer m can be written as a sum of four integral squares

$$m = b_1^2 + b_2^2 + b_3^2 + b_4^2 \tag{2.5}$$

and we have identically

$$(b_1^2 + b_2^2 + b_3^2 + b_4^2)(x_i^2 + x_{i+1}^2 + x_{i+2}^2 + x_{i+3}^2) = y_i^2 + y_{i+1}^2 + y_{i+2}^2 + y_{i+3}^2 \tag{2.6}$$

where

$$\begin{aligned} y_i &= b_1 x_i - b_2 x_{i+1} - b_3 x_{i+2} - b_4 x_{i+3} \\ y_{i+1} &= b_2 x_i + b_1 x_{i+1} - b_4 x_{i+2} + b_3 x_{i+3} \\ y_{i+2} &= b_3 x_i + b_4 x_{i+1} + b_1 x_{i+2} - b_2 x_{i+3} \\ y_{i+3} &= b_4 x_i - b_3 x_{i+1} + b_2 x_{i+2} + b_1 x_{i+3}\,. \end{aligned} \tag{2.7}$$

We note that if we define a matrix B by

$$B = \begin{bmatrix} b_1 & -b_2 & -b_3 & -b_4 \\ b_2 & b_1 & -b_4 & b_3 \\ b_3 & b_4 & b_1 & -b_2 \\ b_4 & -b_3 & b_2 & b_1 \end{bmatrix}, \tag{2.8}$$

then by direct calculation

$$B^{\mathrm{T}}B = BB^{\mathrm{T}}(b_1^2 + b_2^2 + b_3^2 + b_4^2)I. \tag{2.9}$$

From this it follows that $\det B = \pm(b_1^2 + b_2^2 + b_3^2 + b_4^2)^2$ and since b_1^4 has coefficient $+1$ in $\det B$ that $\det B = (b_1^2 + b_2^2 + b_3^2 + b_4^2)^2$. Hence from (2.7) we can express the x's in terms of the y's rationally with denominator m^2, where $m = b_1^2 + b_2^2 + b_3^2 + b_4^2$.

We also note that if $n \equiv 0 \pmod 4$ and if $m = b_1^2 + b_2^2 + b_3^2 + b_4^2$, then we can take a matrix A as the direct sum of $n/4$ copies of B:

$$A = \begin{bmatrix} B & 0 & & 0 \\ 0 & B & & \\ & & \ddots & \\ 0 & & & B \end{bmatrix} \tag{2.10}$$

and from (2.9) it follows that

$$A^{\mathrm{T}}A = AA^{\mathrm{T}} = mI. \tag{2.11}$$

This covers part (iii) of the theorem.

† The arithmetical results used in this section may be found in Hardy and Wright [3].

It remains to consider the cases when $n \equiv 2 \pmod 4$. We can apply (2.6) to the x's in (2.3) four at a time to obtain the identity

$$L_1^2 + \cdots + L_n^2 = y_1^2 + \cdots + y_{n-2}^2 + m(x_{n-1} + x_n^2). \tag{2.12}$$

Here $y_1, \ldots, y_{n-2}$ and x_{n-1}, x_n are independent indeterminates, and $L_1, \ldots, L_n$ are rational linear forms in these indeterminates. We can determine y_1 as a rational linear combination of $y_2, \ldots, y_{n-2}, x_{n-1}, x_n$ by putting

$$L_1 = \pm y_1 \tag{2.13}$$

where we take $L_1 = y_1$ if the coefficient of y_1 in L_i is not $+1$, and putting $L_1 = -y_1$ if it is. Using (2.13) to express y_1 in terms of $y_2, \ldots, y_{n-2}, x_{n-1}, x_n$ we have from (2.12)

$$L_2^2 + \cdots + L_n^2 = y_2^2 + \cdots + y_{n-2}^2 + m(x_{m-1}^2 + x^2), \tag{2.14}$$

an identity with $L_2, \ldots, L_n$ rational linear forms in independent indeterminates $y_2, \ldots, y_{n-2}, x_{n-1}, x_n$. Similarly, we put $L_2 = \pm y_2$ to express y_2 as a rational linear form in $y_3, \ldots, y_{n-2}, x_{n-1}, x_n$. Continuing this process we finally obtain an identity

$$L_{n-1}^2 + L_n^2 = m(x_{n-1}^2 + x_n^2) \tag{2.15}$$

with L_{n-1} and L_n rational linear forms in x_{n-1} and x_n. Taking x_{n-1} and x_n as nonzero multiples of the denominators in L_{n-1} and L_n, we can consider (2.15) as an equation in nonzero integers. From this it follows that m itself is the sum of two integral squares

$$m = a^2 + b^2. \tag{2.16}$$

Conversely, given (2.16) and $n \equiv 2 \pmod 4$ we can define a matrix C of order 2

$$C = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \tag{2.17}$$

and taking A as the direct sum of $n/2$ copies of C we shall have $AA^{\mathrm{T}} = A^{\mathrm{T}}A = mI$. This completes the proof of part (ii) of the theorem including the converse. Thus all parts of the theorem are proved.

3. Rational Completions and Orthogonal Equivalence

Let A be a square matrix of order n and let X be the r by n matrix consisting of the first r rows of A so that

$$A = \begin{bmatrix} X \\ W \end{bmatrix} \tag{3.1}$$

where W is the $n - r$ by n matrix consisting of the last $n - r$ rows of A. Let us

suppose further that every row of W is orthogonal to every row of X. In matrix form this is the condition

$$XW^{\mathrm{T}} = 0. \tag{3.2}$$

Then

$$AA^{\mathrm{T}} = \begin{bmatrix} X \\ W \end{bmatrix} [X^{\mathrm{T}} \quad W^{\mathrm{T}}] = \begin{bmatrix} XX^{\mathrm{T}} & XW^{\mathrm{T}} \\ WX^{\mathrm{T}} & WW^{\mathrm{T}} \end{bmatrix} = \begin{bmatrix} D_1 & 0 \\ 0 & D_2 \end{bmatrix} = D_1 \oplus D_2 . \tag{3.3}$$

The case in which we are particularly interested is that in which $AA^{\mathrm{T}} = mI_n$. Here

$$XX^{\mathrm{T}} = D_1 = mI_r , \qquad WW^{\mathrm{T}} = D_2 = mI_{n-r} . \tag{3.4}$$

The completion problem in which we are interested is the following: *Given an r by n integral matrix X such that $XX^{\mathrm{T}} = mI_r$ can we find an $n - r$ by n matrix W such that $A = \left[\begin{smallmatrix} X \\ W \end{smallmatrix}\right]$ satisfies $AA^{\mathrm{T}} = nI_n$?*

If W is rational, we say that A is a rational completion of X and an integral completion if W is integral.

Providing that the conditions of Theorem 2.1 of the preceding section are satisfied it is immediate from a result of the author and H. J. Ryser [2] that any X satisfying $XX^{\mathrm{T}} = mI_r$ has a rational completion. We quote Theorem 2.1 of that paper.

Theorem (Hall-Ryser) *Suppose that $AA^{\mathrm{T}} = D_1 \oplus D_2$. Here the matrix A is of order n and nonsingular. The matrix D_1 is of order r and D_2 is of order s where $r + s = n$. Let X be an arbitrary r by n matrix such that $XX^{\mathrm{T}} = D_1$. Then there exists an n by n matrix Z having X as its first r rows such that $ZZ^{\mathrm{T}} = D_1 \oplus D_2$. This result holds for all fields F of characteristic $\neq 2$.*

Theorem 3.1 *Suppose that X is an r by n integral matrix satisfying $XX^{\mathrm{T}} = mI_r$, and that m and n satisfy the conditions of Theorem 2.1. Then there is an n by n matrix Z having X as its first r rows and having its last $n - r$ rows rational such that $ZZ^{\mathrm{T}} = mI_n$.*

This follows directly from the Hall–Ryser theorem, taking F as the rational field $D_1 = mI_r$, $D_2 = mI_{n-r}$, and A a solution of $AA^{\mathrm{T}} = mI_n = D_1 \oplus D_2$ which exists since the conditions of Theorem 2.1 are satisfied.

The following theorem is an easy generalization of Theorem 2.2 of the Hall–Ryser paper.

Theorem 3.2 *Suppose that $AA^{\mathrm{T}} = D_1 \oplus D_2$ where A is of order n and nonsingular, and D_1 and D_2 are of order r and $n - r$ and are nonsingular. Suppose further that X and Y are r by n matrices such that $XX^{\mathrm{T}} = YY^{\mathrm{T}} = D_1$. Then there exists an orthogonal matrix U of order n such that $XU = Y$. This result holds for all fields F of characteristic different from 2.*

Proof From the Hall–Ryser theorem there exist n by n matrices R and S such that

$$R = \begin{bmatrix} X \\ W_1 \end{bmatrix}, \qquad S = \begin{bmatrix} Y \\ W_2 \end{bmatrix}$$

with W_1, W_2 $n - r$ by n matrices such that

$$RR^{\mathrm{T}} = D_1 \oplus D_2, \qquad SS^{\mathrm{T}} = D_1 \oplus D_2. \tag{3.5}$$

Putting $U = R^{-1}S$ it follows from (3.5) that $UU^{\mathrm{T}} = I$ or that U is orthogonal. Then

$$\begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} RU = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} S \tag{3.6}$$

or

$$XU = Y, \tag{3.7}$$

which is the conclusion of the theorem.

4. Results on Integral Completions

Theorem 4.1 *Suppose that m and n satisfy the conditions of Theorem* 2.1. *Then if* $r = n - 1$ *or* $n - 2$ *and* X *is an integral* r *by* n *matrix satisfying* $XX^{\mathrm{T}} = mI_r$ *there is an* n *by* n *integral matrix* A *having* X *as its first* r *rows such that* $AA^{\mathrm{T}} = mI_n$.

Proof For $r = n - 1$, the result is easy. Let A be a rational completion having X as its first $n - 1$ rows, whose existence is given by Theorem 3.1. Then in fact A is an integral matrix.

$$A = [a_{ij}], \qquad AA^{\mathrm{T}} = mI_n, \qquad A^{\mathrm{T}}A = mI_n. \tag{4.1}$$

The last follows since $mA^{-1} = A^{\mathrm{T}}$, and yields

$$\sum_i a_{ij}^2 = m, \qquad j = 1, \ldots, n. \tag{4.2}$$

But $a_{1j}, a_{2j}, \ldots, a_{n-1\,j}$ are integers as entries in X. Hence a_{nj}^2 is an integer but as a_{nj} is rational it follows that a_{nj} is an integer for $j = 1, \ldots, n$. Thus A is an integral matrix and so is an integral completion of X.

Now suppose $r = n - 2$ and let Z be a rational completion of X as given by Theorem 3.1. Then

$$ZZ^{\mathrm{T}} = mI_n, \qquad Z^{\mathrm{T}}Z = mI_n. \tag{4.3}$$

Here the first $n - 2$ rows of Z are integral, and the last two are rational. Let s be the smallest positive integer such that $sZ = A_1$ is an integral matrix. Then

$$A_1 A_1^{\mathrm{T}} = A_1^{\mathrm{T}} A = s^2 mI_n. \tag{4.4}$$

Here if $X = [a_{ij}]$, $i = 1, \ldots, n-2$, $j = 1, \ldots, n$, A_1 has the shape

$$A_1 = \begin{bmatrix} sa_{11} & \cdots & sa_{1j} & \cdots & sa_{1n} \\ sa_{21} & \cdots & sa_{2j} & \cdots & sa_{2n} \\ \vdots & & \vdots & & \vdots \\ sa_{n-21} & \cdots & sa_{n-2j} & \cdots & sa_{n-2n} \\ x_1 & \cdots & x_j & \cdots & x_n \\ y_1 & \cdots & y_j & \cdots & y_n \end{bmatrix} \tag{4.5}$$

where all entries are integral. Clearly if $s = 1$, then A_1 is an integral completion of X. We shall show that the least positive s giving a matrix such as A_1 is $s = 1$. From $A_1^{\mathrm{T}} A_1 = s^2 m I_m$ we have

$$\begin{aligned} s^2(a_{1j}^2 + \cdots + a_{n-2j}^2) + x_j^2 + y_j^2 &= s^2 m, \qquad j - 1, \ldots, n \\ s^2(a_{1j}a_{1k} + \cdots + a_{n-2j}a_{n-2k}) + x_j x_k + y_j y_k &= 0, \qquad j \neq k. \end{aligned} \tag{4.6}$$

Let p be a prime dividing s. Then (4.6) gives

$$\begin{aligned} x_j^2 + y_j^2 \equiv 0 \pmod{p^2}, \qquad x_j x_k + y_j y_k \equiv 0 \pmod{p^2}, \\ j, k = 1, \ldots, n, \quad j \neq k. \end{aligned} \tag{4.7}$$

Then if $p = 2$ or $p \equiv 3 \pmod 4$ it follows from (4.7) that

$$x_j \equiv y_j \equiv 0 \pmod{p}, \qquad j = 1, \ldots, n. \tag{4.8}$$

In this case $p^{-1}A_1 = A_2$ is comparable to A_1 with $s = ps_1$ replaced by s_1. We may suppose that $p \mid n$ but that p does not divide every x and y in A_1. Choose j so that p does not divide both x_j and y_j. Then from (4.7) p divides neither x_j nor y_j.

$$x_j^2 + y_j^2 \equiv 0 \pmod{p^2}, \qquad x_j \not\equiv 0 \ (p), \quad y_j \not\equiv 0 \ (p). \tag{4.9}$$

As $p \neq 2$, $p \not\equiv 3 \pmod 4$ it follows that p is a sum of two squares and is not a prime in the Gaussian integers

$$p = a^2 + b^2 = (a + bi)(a - bi). \tag{4.10}$$

From (4.9)

$$(x_j + y_j i)(x_j - y_j i) \equiv 0 \ (\mathrm{mod}(a + bi)^2(a - bi)^2). \tag{4.11}$$

Since $x_j, y_j \not\equiv 0 \pmod p$, it follows that $x_j + y_j i$ is not divisible by both of $a + bi$ and $a - bi$ and also that $x_j - y_j i$ is not divisible by both of $a + bi$ and $a - bi$. Let us suppose the notation such that $(x_j + y_j i, a - bi) = 1$. Then $(a + bi)^2 = (a^2 - b^2 + 2abi) = d + ei$ divides $x_j + y_j i$, where $d^2 + e^2 = p^2$. Then

$$x_j + y_j i = (d + ei)(w_j + z_j i) \tag{4.12}$$

with w_j and z_j rational integers. It follows that

$$(d - ei)(x_j + y_j i) = (dx_j + ey_j) + (-ex_j + dy_j)i = p^2 w_j + p^2 z_j . \quad (4.13)$$

Now consider for $k \neq j$ the identity

$$(x_j x_k + y_j y_k)^2 + (x_j y_k - x_k y_j)^2 = (x_j^2 + y_j^2)(x_k^2 + y_k^2). \quad (4.14)$$

From (4.7) we have $x_j^2 + y_j^2$, $x_k^2 + y_k^2$, $x_j x_k + y_j y_k$ all multiples of p^2 so that from (4.14) $x_j y_k - x_k y_j$ is also a multiple of p^2.

Now consider the product

$$(x_j - y_j i)(x_k - y_k i) = (x_j y_k + y_j y_k) + (-x_j y_k + x_k y_j)i = p^2 u + p^2 v i. \quad (4.15)$$

Since $(x_j + y_j i, a - bi) = 1$ and $p^2 = (a + bi)^2(a - bi)^2$ it follows that $(a - bi)^2 = d - ei$ divides $x_k - y_k i$. Hence for the conjugates $d + ei$ divides $x_k + y_k i$. Thus

$$x_k + y_k i = (d + ei)(w_k + z_k i) \quad (4.16)$$

with w_k and z_k rational integers. Then

$$(d - ei)(x_k + y_k i) = (dx_k + ey_k)(-ex_k + dy_k)i = p^2 w_k + p^2 z_k i. \quad (4.17)$$

Now write $s = ps_1$ and define the matrix M_p by

$$M_p = \left[\begin{array}{c|cc} pI_{n-2} & & \\ \hline & d & e \\ & -e & d \end{array}\right] \quad (4.18)$$

It is immediate that $M_p M_p^{\mathrm{T}} = p^2 I_n$. Using (4.13) and (4.17) for $k \neq j$, we have

$$M_p A_1 = \left[\begin{array}{c|cc} pI_{n-2} & & \\ \hline & d & e \\ & -e & d \end{array}\right] \left[\begin{array}{c} ps_1 X \\ \hline x_1 \quad x_j \quad x_n \\ y_1 \quad y_j \quad y_n \end{array}\right]$$

$$= \left[\begin{array}{c} p^2 s_1 X \\ \hline dx_1 + ey_1 \cdots dx_j + ey_s \cdots dx_k + ey_k \cdots dx_n + ey_n \\ -ex_1 + dy_1 \cdots -ex_j + dy_j \cdots -ex_k + dy_k \cdots -ex_n + dy_n \end{array}\right]$$

$$= \left[\begin{array}{c} p^2 s_1 X \\ \hline p^2 w_1 \cdots p^2 w_j \cdots p^2 w_k \cdots p^2 w_n \\ p^2 z_1 \cdots p^2 x_j \cdots p^2 z_k \cdots p^2 z_n \end{array}\right]$$

$$= p^2 \left[\begin{array}{c} s_1 X \\ \hline w_1 \cdots w_j \cdots w_n \\ z_1 \cdots z_j \cdots z_n \end{array}\right] = p^2 A_2 . \quad (4.19)$$

Here A_2 is an integral matrix with the properties of A_1, but with $s = ps_1$ replaced by the smaller s_1. Hence the smallest s appearing in such an A must be $s = 1$ and in this case A is an integral completion of X, proving our theorem.

Theorem 4.2 *If m and n are integers satisfying conditions of Theorem* 2.1 *and if X is an r by n integral matrix satisfying $XX^{\mathrm{T}} = mI_r$, then if $n \leq 4$ there is always an integral completion A of order n with X as its first r rows such that $AA^{\mathrm{T}} = mI_n$.*

Proof This is essentially a corollary of Theorem 4.1 which covers all cases with $n \leq 4$ except for $r = 1$, $n = 4$. But in this case taking X as the first row of a matrix B as in (2.8) we have an integral completion of X.

5. Integral Completions for Hadamard Matrices

A Hadamard matrix $H = [h_{ij}]$, $i, j = 1, \ldots, n$ is a square matrix with every entry $h_{ij} = \pm 1$ such that

$$HH^{\mathrm{T}} = nI_n, \qquad H^{\mathrm{T}}H = nI_n. \tag{5.1}$$

These two conditions are equivalent as both of them assert that $nH^{-1} = H^{\mathrm{T}}$. It is well known that for a Hadamard matrix $n = 1, 2$ or $n \equiv 0 \pmod 4$. The natural question here is whether or not given an r by n matrix X with every entry ± 1 such that

$$XX^{\mathrm{T}} = nI_r \tag{5.2}$$

does there exist a Hadamard matrix H with X as its first r rows?

Leaving the cases $n = 1, 2$ as exercises for the reader, we shall assume $n \equiv 0 \pmod 4$ so that the conditions of Theorem 2.1 are automatically satisfied.

Theorem 5.1 *Let X be an r by n matrix, $n \equiv 0 \pmod 4$ with every entry $+1$ or -1 satisfying* 5.2. *Then if $r = n - 1$, $n - 2$, $n - 3$, or $n - 4$ there is a Hadamard matrix of order n with X as its first r rows.*

Proof Let H_1 be a rational completion of X. Then $H_1H_1^{\mathrm{T}} = H_1^{\mathrm{T}}H_1 = nI_n$ so that in $H_1 = [h_{ij}]$ we have

$$\sum_{t=1}^{n} h_{tj}^2 = n, \qquad \sum_{t=1}^{n} h_{tj}h_{tk} = 0, \qquad j, k = 1, \ldots, n, \quad j \neq k. \tag{5.3}$$

It follows that

$$\sum_{t=r+1}^{n} h_{tj}^2 = n - \sum_{t=1}^{r} h_{tj}^2 = n - r, \qquad j = 1, \ldots, n \tag{5.4}$$

and

$$\sum_{t=r+1}^{n} h_{ij}h_{tk} = -\sum_{t=1}^{r} h_{ij}h_{tk} = \sum_{t=1}^{r} \pm 1 \equiv r \pmod 2. \tag{5.5}$$

In finding a completion for X it is clear that we may permute the rows of X or change signs of some of them without altering the final rows of the completion. Also if we permute the columns of X and change the signs of some of them, if we perform the same operations on the columns of the final rows, we shall still have a completion. Since these operations take integral completions into integral completions and are reversible, we may use them freely in deciding whether or not a specified X has a completion.

If Y and Z are two rational q by $n-r$ matrices with $YY^{\mathrm{T}} = ZZ^{\mathrm{T}}$ a nonsingular matrix, then by Theorem 3.2 there exists a unitary matrix U of order $n-r$ such that $YU = Z$. Taking transposes we have $U^{\mathrm{T}}Y^{\mathrm{T}} = Z^{\mathrm{T}}$. Hence we may define H_1^* by

$$H_1^* = \left[\begin{array}{c|c} I_r & 0 \\ \hline 0 & U^{\mathrm{T}} \end{array}\right]\left[\begin{array}{c} X \\ \hline W \end{array}\right] = \left[\begin{array}{c} X \\ \hline U^{\mathrm{T}}W \end{array}\right]. \tag{5.6}$$

Then H_1^* is also a rational completion of X and if the first q columns of W are the matrix Y^{T}, then the first q columns of $U^{\mathrm{T}}W$ are the matrix Z^{T}. This is very useful since in the cases we shall consider we can replace rational columns Y^{T} by integral columns Z^{T} and obtain an integral completion.

First, if $r = n-1$ from (5.4) in the rational completion H_1 we have $h_{nj}^2 = 1$, $j = 1, \ldots, n$, and so $h_{nj} = \pm 1$, $j = 1, \ldots, n$, and thus $H_1 = H$ is the completion which is a Hadamard matrix.

If $r = n-2$ write H_1 in the form

$$H_1 = \left[\begin{array}{c} X \\ \hline x_1 \quad x_2 \quad \cdots \quad x_n \\ y_1 \quad y_2 \quad \cdots \quad y_n \end{array}\right]. \tag{5.7}$$

Here (5.4) and (5.5) give

$$x_j^2 + y_j^2 = 2, \quad j = 1, \ldots, n, \qquad x_jx_k + y_jy_k = 2s, \quad j \neq k \tag{5.8}$$

where $2s$ is some even integer and since $(x_j \pm x_k)^2 + (y_j \pm y_k)^2 \geq 0$ we have $-2 \leq x_jx_k + y_jy_k \leq 2$.

By Theorem 3.2 as $x_1^2 + y_1^2 = 2$ we can apply (5.6) to replace H_1 by a completion H_1^* in which $(x_1, y_1) = (1, 1)$, and without loss of generality assume this to be the case in H_1. Thus from (5.8) with $j \neq 1$ and $k = 1$

$$x_j^2 + y_j^2 = 2, \qquad x_j + y_j = -2, 0, 2. \tag{5.9}$$

If $x_j + y_j = 2$, then

$$(x_j - 1)^2 + (y_j - 1)^2 = 2 - 4 + 2 = 0 \tag{5.10}$$

and $x_j = 1$, $y_j = 1$. Similarly if $x_j + y_2 = -2$, then

$$(x_j + 1)^2 + (y_j + 1)^2 = 2 - 4 + 2 = 0 \tag{5.11}$$

and $x_j = -1$, $y_j = -1$.

If $x_j + y_j = \pm 2$ for all j, then from (5.10) and (5.11) the last two rows are identical. This is impossible since the inner product of the last two rows is zero. Hence for some j we have $x_j + y_j = 0$ and then

$$x_j^2 + y_j^2 = 2, \qquad x_j + y_j = 0, \qquad 2x_j^2 = 2, \qquad x_j = \pm 1, \qquad y_j = \mp 1$$

Thus without loss of generality, we may take $x_2 = 1$, $y_2 = -1$. Now H_1 has the form

$$H_1 = \left[\begin{array}{cccccc} & & & X & & \\ \hline 1 & 1 & \cdots & x_j & \cdots & x_n \\ 1 & -1 & \cdots & y_j & \cdots & y_n \end{array}\right]. \tag{5.12}$$

Here for $j > 2$ we have from (5.9) with $k = 1$ and $k = 2$

$$x_j^2 + y_j^2 = 2, \qquad x_j + y_j = 0, \pm 2, \qquad x_j - y_j = 0, \pm 2. \tag{5.13}$$

Here the only possibilities are $(x_j, y_j) = (1, 1)$, $(-1, -1)$, $(1, -1)$, and $(-1, 1)$. Hence $H - H_1$ has every entry ± 1 and so is a Hadamard matrix. We might also have appealed to Theorem 4.1 and taken H_1 as an integral completion of X and then $x_j^2 + y_j^2 = 2$ would give $x_j = \pm 1$, $y_j = \pm 1$, and so H_1 is an Hadamard matrix.

Now take $r = n - 3$ and write the rational completion H_1 in the form

$$H_1 = \left[\begin{array}{cccccc} & & & X & & \\ \hline x_1 & \cdots & x_j & \cdots & x_n \\ y_1 & \cdots & y_j & \cdots & y_n \\ z_1 & \cdots & z_j & \cdots & z_n \end{array}\right].$$

Here (5.4) and (5.5) give

$$x_j^2 + y_j^2 + z_j^2 = 3, \qquad x_j x_k + y_j y_k + z_j z_k = -3, -1, 1, 3,$$
$$j, k = 1, \ldots, n, \quad j \neq k \tag{5.14}$$

since $x_j x_k + y_j y_k + z_j z_k$ is an odd integer in absolute value at most 3.

Since $x_1^2 + y_1^2 + z_1^2 = 3$ by Theorem 3.2 we may apply (5.6) to replace (x_1, y_1, z_1) by $(1, 1, 1)$, and assume this to be the case in (5.13). Then from (5.14) with $j \neq 1$ and $k = 1$ we have

$$x_j^2 + y_j^2 + z_j^2 = 3, \qquad x_j + y_j + z_j = -3, -1, 1, 3. \tag{5.15}$$

If $x_j + y_j + z_j = 3$, then $(x_j - 1)^2 + (y_j - 1)^2 + (z_j - 1)^2 = 0$ and $(x_j, y_j, z_j) = (1, 1, 1)$ and similarly if $x_j + y_j + z_j = -3$, then $(x_j, y_j, z_j) = (-1, -1, -1)$. Hence unless $x_j + y_j + z_j = \pm 1$ for some j, the last three rows are identical, which conflicts with their inner products being zero. Without loss of generality take $j = 2$ and $x_2 + y_2 + z_2 = 1$. Then defining Y and Z by

$$Y = \begin{bmatrix} 1 & 1 & 1 \\ x_2 & y_2 & z_2 \end{bmatrix}, \qquad Z = \begin{bmatrix} 1 & 1 & 1 \\ -1 & 1 & 1 \end{bmatrix}, \tag{5.16}$$

we have

$$YY^{\mathrm{T}} = Z, \qquad Z^{\mathrm{T}} = \begin{bmatrix} 3 & 1 \\ 1 & 3 \end{bmatrix}. \tag{5.17}$$

Hence from Theorem 3.2 there is a rational orthogonal matrix U with $YU = Z$. Hence applying (5.6) we have a rational completion H_1^* with $(x_1, y_1, z_1) = (1, 1, 1)$ and $(x_2, y_2, z_2) = (-1, 1, 1)$ which we may assume to hold in H_1.

Then with $j > 2$ and $k = 1$ and 2 (5.14) becomes

$$x_j^2 + y_j^2 + z_j^2 = 3, \qquad x_j + y_j + z_j = \pm 1, \pm 3,$$
$$-x_y + y_j + z_j = \pm 1, \pm 3. \tag{5.18}$$

We note that if the inner product of two columns of the last three rows is $+3$, then the columns are identical, while if the inner product is -3 then they are negatives of each other. If this held for every $j > 2$, then the last two rows would be identical, a conflict. Thus for certain j's

$$x_j + y_j + z_j = \varepsilon_1 = \pm 1, \qquad -x_j + y_j + z_j = \varepsilon_2 = \pm 1. \tag{5.19}$$

If $\varepsilon_1 = \varepsilon_2$, then $x_j = 0$; while if $\varepsilon_1 = -\varepsilon_2$, then $x_j = \varepsilon_1$. Hence every x_j, $j = 1, \ldots, n$ is 0 or ± 1. But since $x_1^2 + \cdots + x_n^2 = n$, the alternative $x_j = 0$ cannot arise and $x_j = \pm 1, j = 1, \ldots, n$. We can now add the row $x_1, \ldots, x_n$ to X to get X' and by our previous proof complete X' with two more rows to a Hadamard H. But we may also proceed directly taking $j = 3, \varepsilon_1 = 1$ without loss of generality. Then with

$$Y = \begin{bmatrix} 1 & 1 & 1 \\ -1 & 1 & 1 \\ x_3 & y_3 & z_3 \end{bmatrix} \quad \text{and} \quad Z = \begin{bmatrix} 1 & 1 & 1 \\ -1 & 1 & 1 \\ 1 & 1 & -1 \end{bmatrix} \tag{5.20}$$

we have

$$YY^{\mathrm{T}} = ZZ^{\mathrm{T}} = \begin{bmatrix} 3 & 1 & 1 \\ 1 & 3 & -1 \\ 1 & -1 & 3 \end{bmatrix} \tag{5.21}$$

and with $U = Y^{-1}Z$ apply (5.6) to replace (x_3, y_3, z_3) by $(1, 1, -1)$. Here

$$H_1 = \left[\begin{array}{cccccc} & & & X & & \\ \hline 1 & -1 & 1 & \cdots & x_j & x_n \\ 1 & 1 & 1 & \cdots & y_j & y_n \\ 1 & 1 & -1 & \cdots & z_j & z_n \end{array}\right], \tag{5.22}$$

and we assert that H_1 is a Hadamard matrix. For we have for $j > 3$,

$$\begin{gathered} x_j^2 + y_j^2 + z_j^2 = 3, \\ x_j + y_j + z_j = \pm 1, \pm 3, \qquad -x_j + y_j + z_j = \pm 1, \pm 3, \\ x_j + y_j - z_j = \pm 1, \pm 3. \end{gathered} \tag{5.23}$$

If we have ± 3 in any one of these cases, the jth column is equal to one of the first three or its negative. There remains

$$\begin{gathered} x_j + y_j + z_j = \varepsilon_1 = \pm 1, \qquad -x_j + y_j + z_j = \varepsilon_2 \pm 1, \\ x_j + y_j - z_j = \varepsilon_3 = \pm 1. \end{gathered} \tag{5.24}$$

As observed earlier we must have $\varepsilon_1 = -\varepsilon_2$ and $x_j = \varepsilon_1$. Similarly, if $\varepsilon_1 = \varepsilon_3$, we have $z_j = 0$; while if $\varepsilon_1 = -\varepsilon_3$, we have $z_j = \varepsilon_1$. And since we must exclude $z_j = 0$, we have $\varepsilon_2 = -\varepsilon_1$, $\varepsilon_3 = -\varepsilon_1$, and

$$(x_j, y_j, z_j) = (1, -1, 1) \quad \text{or} \quad (-1, 1, -1). \tag{5.25}$$

Hence every x, y, and z is ± 1 and the completion of (5.22) is a Hadamard matrix.

The case with $r = n - 4$ is more difficult to handle: We write a rational completion H_1 as

$$H_1 = \left[\begin{array}{ccccc} & & X & & \\ \hline x_1 & \cdots & x_j & \cdots & x_n \\ y_1 & \cdots & y_j & \cdots & y_n \\ z_1 & \cdots & z_j & \cdots & z_n \\ w_1 & \cdots & w_j & \cdots & w_n \end{array}\right]. \tag{5.26}$$

From (5.4) and (5.5) we have

$$x_j^2 + y_j^2 + z_j^2 + w_j^2 = 4, \qquad x_j x_k + y_j y_k + z_j z_k + w_j w_k = 0, \pm 2, \pm 4. \tag{5.27}$$

We subdivide the proof into two subcases. In the first subcase we assume that only the inner products $0, \pm 4$ arise. We may apply Theorem 3.2 and (5.6) to replace (x_1, y_1, z_1, w_1) by $(1, 1, 1, 1)$. If the jth column has inner product ± 4 with the first column, it will be the same as the first column or its negative. Since the last four rows are not identical, there will be a j for which $x_j + y_j + z_j + w_j = 0$, which we may take to be $j = 2$. Then from Theorem 3.2 and (5.6) we may replace the first two columns by $(1, 1, 1, 1)$ and $(1, 1, -1, -1)$. Since the last two rows cannot be identical, there must be a column whose inner product is not ± 4 with either of these, and by our assumption this means a column whose inner product is zero with both of these. Without loss we may take this to be the third column and by Theorem 3.2 and (5.6) replace (x_3, y_3, z_3, w_3) by $(1, -1, 1, -1)$. Now H_1 is in the form

$$H_1 = \left[\begin{array}{ccccccc} & & & X & & & \\ \hline 1 & 1 & 1 & \cdots & x_j & \cdots & x_n \\ 1 & 1 & -1 & \cdots & y_j & \cdots & y_n \\ 1 & -1 & 1 & \cdots & z_j & \cdots & z_n \\ 1 & -1 & -1 & \cdots & w_j & \cdots & w_n \end{array}\right]. \tag{5.28}$$

Now we assert that H_1 is a Hadamard matrix. For $x_j^2 + y_j^2 + z_j^2 + w_j^2 = 4$ and if this column has inner product ± 4 with one of the first three, it is equal to that column or its negative. But if it has inner product zero with all three of the first, then we find $(x_j, y_j, z_j, w_j) = (1, -1, -1, 1)$ or $(-1, 1, 1, -1)$ since $x_j = -y_j = -z_j = w_j$ from the vanishing of the inner products. Hence in the first subcase there is a completion that is a Hadamard matrix.

In the second subcase there will be an inner product ± 2. Without loss we may take this to be $+2$ and the inner product of the first two columns. Hence by Theorem 3.2 and (5.6) we may take H_1 in the form

$$H_1 = \left[\begin{array}{cccccc} & & X & & & \\ \hline 1 & -1 & \cdots & x_j & \cdots & x_n \\ 1 & 1 & \cdots & y_j & \cdots & y_n \\ 1 & 1 & \cdots & z_j & \cdots & z_n \\ 1 & 1 & \cdots & w_j & \cdots & w_n \end{array}\right]. \tag{5.29}$$

Now let us change the signs of rows of X to make the first column consist entirely of $+1$'s. Since the inner product of the first two columns of H_1 is zero, writing $n = 4t$ we find in X

$$2t - 3 \text{ rows, } 1, 1, \ldots, 2t - 1 \text{ rows } 1, -1, \ldots. \tag{5.30}$$

In X we shall subdivide these rows according whether the entry in

column j is $+1$ or -1

$$\begin{array}{lccc} \text{column} & 1, & 2, & j \\ a \text{ rows} & 1 & 1 & 1 \\ b \text{ rows} & 1 & 1 & -1 \\ c \text{ rows} & 1 & -1 & 1 \\ d \text{ rows} & 1 & -1 & -1 \end{array} \tag{5.31}$$

From (5.30) we have

$$a + b = 2t - 3, \qquad c + d = 2t - 1. \tag{5.32}$$

We now calculate the inner product of the jth column c_j with the first and second columns c_1 and c_2:

$$\begin{aligned} (c_1, c_j) &= a - b + c - d + x_j + y_j + z_j + w_n = 0 \\ (c_2, c_j) &= a - b - c + d - x_j + y_j + z_j + w_j = 0 \end{aligned} \tag{5.33}$$

It now follows that

$$x_j = -c + d = 2t - 1 - 2c. \tag{5.34}$$

Hence x_j is an odd integer and as $x_j^2 + y_j^2 + z_j^2 + w_j^2 = 4$ that necessarily $x_j = \pm 1$. We may now adjoin the row of x's to X to form X' an $n - 3$ by n matrix of ± 1's and by our previous case there is a Hadamard matrix H that is a completion of X'. This completes the proof of the second subcase for $r = n - 4$ and so all parts of the theorem.

It is not true that every X with entries ± 1 satisfying (5.2) can be completed to a Hadamard matrix. We shall show what some of these X's are. There is, up to equivalence of permuting rows and columns, and changing signs of rows and columns an unique Hadamard matrix H_4 of order 4:

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}. \tag{5.35}$$

If we take the tensor product of $e_t = (1, \ldots, 1)$ with t 1's, t being odd, with H_4 we have an X,

$$X = \begin{bmatrix} 1 \cdots 1 & 1 \cdots 1 & 1 \cdots 1 & 1 \cdots 1 \\ 1 \cdots 1 & 1 \cdots 1 & -1 \cdots -1 & -1 \cdots -1 \\ 1 \cdots 1 & -1 \cdots -1 & 1 \cdots 1 & -1 \cdots -1 \\ 1 \cdots 1 & -1 \cdots -1 & -1 \cdots -1 & 1 \cdots 1 \end{bmatrix} \tag{5.36}$$

where X is a 4 by $4t$ matrix such that $XX^{\mathrm{T}} = 4tI_4$.

Since H_4 in (5.35) is normalized so that first column consists entirely of

$+1$'s and since the columns are orthogonal, the sum of the entries in every other column is zero. Hence the sum of the four rows of H_4 is the vector $(4, 0, 0, 0)$. Correspondingly the sum of the four rows of X is $(4e_t, 0, 0, 0)$. Consequently, a vector $(x_1, \ldots, x_t, \ldots, x_{4t})$ in which every $x_i = \pm 1$ cannot be orthogonal to all four rows X since then it would be orthogonal to their sum $(4e_t, 0, 0, 0)$ and then in $(x_1, \ldots, x_t)$ half the entries would have to be $+1$ and other half -1. But with t odd, this is impossible. In the same way the tensor product of e_t with any Hadamard matrix H_{4m} of order $4m$ will give an X that is $4m$ by $4mt$ which cannot be completed to a Hadamard matrix H_{4mt} since the existence of a completion of X is independent of the normalization of H_{4m}.

In the light of these observations the matrix A (5.37) is of interest.

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ 2 & -2 & 0 & 1 & -1 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 2 & 0 & -2 & -1 & 1 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & -2 & 1 & -1 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & -1 & 0 & 1 & 2 & -2 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 1 & 0 & -1 & 2 & 0 & -2 \\ 0 & 0 & 0 & 1 & 0 & -1 & -1 & 0 & 1 & 0 & 2 & -2 \\ 0 & 0 & 0 & -1 & 2 & -1 & 1 & -2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & -1 & 2 & -1 & -1 & 2 & 0 & 0 & 0 \end{bmatrix}. \qquad (5.37)$$

Here $AA^{\mathrm{T}} = A^{\mathrm{T}}A = 12I$ so that although the first four rows X of A are such that they cannot be extended to a Hadamard matrix, nevertheless A is an integral completion of X.

REFERENCES

[1] S. Chowla and H. J. Ryser, Combinatorial problems, *Canad. J. Math.* **2** (1950), 93–99.

[2] Marshall Hall and H. J. Ryser, Normal completions of incidence matrices, *Amer. J. Math.* **76** (1954), 581–589.

[3] G. H. Hardy and E. M. Wright, "The Theory of Numbers." Oxford University Press, London and New York, 1938.

AMS (MOS) 1970 subject classifications: 05B20, 15A36.

Lie Algebraic Proofs of Some Theorems on Partitions

J. W. B. HUGHES

QUEEN MARY COLLEGE
LONDON, ENGLAND

An analysis is given of the layer structure of fundamental representations of the simple Lie algebras, expressions being given for the multiplicities of the layers in terms of the partitions $(j; l, i)$, $P(j; n, n)$, *and* $Q(j'; a, b, c)$. *A general theorem due to E. B. Dynkin concerning the layer structure is then used to derive certain properties of these partitions; a typical example is the result* $P(j; n, n) \geq P(j-1; n, n)$ *for* $j \leq [\frac{1}{4}n(n+1)]$.

1. Introduction

In a previous paper [1] a proof was given of a theorem on the partition function $(j; n-i, i)$ of an integer j into at most $n-i$ integers none of which exceeds i, namely that, for $0 \leq j \leq [i(n-i)/2]$, $(j; n-i, i) \geq (j-1; n-i, i)$; the connection of this theorem to the layer structure of fundamental representations of the Lie algebra $A(n-1)$ was also mentioned. The proof was unfortunately quite erroneous,‡ and in fact properties of this nature appear to be quite difficult to prove using conventional means (see for instance Chowla [2, unsolved problem 68] and Szekeres [3, 4]). However, by a reversal of the argument, known properties of the structure of these representations could be used to give a Lie algebraic proof of the above theorem. The

‡ I am indebted to Professor G. E. Andrews of Pennsylvania State University for pointing this out to me.

theorem was in fact already proved by Elliott [5] using invariant theory of quantics, but by considering the layer structure of representations of the other simple Lie algebras, new theorems concerning different partitions can also be derived.

It is the purpose of this paper, therefore, to give the analysis of the fundamental representations of $A(n-1)$, $B(n)$, $C(n)$, and $D(n)$, and in particular to calculate the multiplicities of the jth layers of these representations. In all cases they are found to equal certain partition functions, the above $(j; n-i, i)$ for $A(n-1)$, the partition function $P(j; n, n)$ of j into at most n strictly decreasing integers none of which exceeds n in the case of the nth fundamental representation of $B(n)$ and the $(n-1)$th and nth fundamental representation of $D(n)$. For the cases of the other fundamental representations of $B(n)$, $C(n)$, and $D(n)$, these multiplicities are given in terms of the partition function $Q(j'; a, b, c)$ which denotes the number of partitions of j' into exactly a strictly increasing integers none of which exceeds b and in which c of the integers contribute negatively.

Using a theorem by Dynkin [6], which states that these layers are "spindle shaped," five theorems, each in two parts, are derived. The first part of each theorem is trivial and can be derived very simply, in the first two cases from elementary properties of the appropriate generating functions, and in the other cases from the obvious relation

$$Q(j'; a, b, c) = Q(-j'; a, b, a-c). \tag{1}$$

The second parts of the theorems, on the other hand, do not appear to be easily derivable using conventional methods and are, as far as the author is aware, with the exception of Theorem 1b, all quite new. Theorem 1 concerns $(j; n-i, i)$; Theorem 2 concerns $P(j; n, n)$; and Theorems 3–5 concern $Q(j'; a, b, c)$.

Before giving these Lie algebraic derivations, in order to place the results of this paper in perspective we show how some elementary properties of the above partitions can be derived using their generating functions. For $(j; n-i, i)$ the generating function is the Gaussian polynomial

$$\begin{bmatrix} n \\ i \end{bmatrix}(q) \equiv \frac{(1-q^n)\cdots(1-q^{n-i+1})}{(1-q^i)\cdots(1-q)} = \sum_{j=0}^{i(n-i)} (j; n-i, i)q^j \tag{2}$$

(see Hardy and Wright [7], Rademacher [8]) where one conventionally defines $\begin{bmatrix} n \\ 0 \end{bmatrix}(q) = 1$. The Gaussian polynomials are reciprocal and satisfy [8]

$$\begin{bmatrix} n \\ i \end{bmatrix}(1) = \binom{n}{i}. \tag{3}$$

The reciprocal nature of $\begin{bmatrix} n \\ i \end{bmatrix}(q)$ will turn out to be precisely the content of Theorem 1a. Also, the use of (3) in (2) gives

$$\sum_{j=1}^{i(n-i)} (j; n-i, i) = \binom{n}{i}, \tag{4}$$

which, as we shall see in Section 2, states that the ith fundamental representation of $A(n-1)$ has dimension $\binom{n}{i}$.

The generating function for $P(j; n, n)$ is

$$\sum_{r=0}^{n} q^{r(r+1)/2} \begin{bmatrix} n \\ r \end{bmatrix}(q) = (1+q)(1+q^2)\cdots(1+q^n)$$

$$= \sum_{j=0}^{n(n+1)/2} P(j; n, n) q^j. \tag{5}$$

Theorem 2a will turn out to be the statement that this, too, is a reciprocal polynomial. Also, putting $q = 1$ in (5) gives

$$\sum_{j=0}^{n(n+1)/2} P(j; n, n) = \sum_{r=0}^{n} \binom{n}{r} = 2^n, \tag{6}$$

which states (see Section 3) that the nth fundamental representation of $B(n)$ has dimension 2^n.

Finally, for $Q(j'; a, b, c)$ we have the generating function‡

$$\prod_{r=1}^{b} (1 + xq^r + xtq^{-r}) = \sum_{a,\, c \geq 0} \sum_{j' = -\infty}^{\infty} Q(j'; a, b, c) x^a t^c q^{j'}. \tag{7}$$

It is worth noting here that while $Q(j'; a, b, c)$ arises naturally in the context of this paper, its definition as a partition function is somewhat artificial. However, let $Q^*(j'; a, b, c)$ denote the number of partitions of j' with each part no larger than b, with no part appearing more than twice, with a parts appearing exactly once, and with c integers used as parts. Then

$$Q\left(j' - \binom{b+1}{2}; b-a, b, b-c\right) = Q^*(j'; a, b, c). \tag{8}$$

This is obvious from the following elementary identities:

$$\sum Q\left(j' - \binom{b+1}{2}; b-a, b, b-c\right) x^a t^c q^{j'}$$

$$= q^{\binom{b+1}{2}} x^b t^b \sum Q\left(j' - \binom{b+1}{2}; a, b, c\right) x^{-a} t^{-c} q^{j'}$$

$$= q^{\binom{b+1}{2}} x^b t^b \prod_{r=1}^{b} (1 + x^{-1}q^r + x^{-1}t^{-1}q^{-r})$$

$$= \prod_{r=1}^{b} q^r xt (1 + x^{-1}q^r + x^{-1}t^{-1}q^{-r})$$

$$= \prod_{r=1}^{b} (1 + xtq^r + tq^{2r}) = \sum Q^*(j'; a, b, c) x^a t^c q^{j'}. \tag{9}$$

‡ I should like to thank the referee for pointing this out to me.

Thus Q is only a superficially altered Q^*, and Q^* is a very natural partition function.

If in Eq. (7) we put $q = 1$ and equate coefficients of $x^a t^c$, we obtain

$$\sum_{j=-\infty}^{\infty} Q(j; a, b, c) = \binom{b}{a}\binom{a}{c}. \tag{10}$$

This result, as we shall see later, may be used to calculate the number of distinct weights belonging to shells of fundamental representations of the Lie algebras $B(n)$, $C(n)$, and $D(n)$.

In dealing with $A(n-1)$ in Section 2, we also summarize, without proofs, those properties of simple Lie algebras that are needed in order to calculate the layer multiplicities. The Lie algebras $B(n)$, $C(n)$, and $D(n)$ are treated more briefly in Sections 3, 4, and 5, respectively.

2. $A(n-1)$

In this section we consider the case of $A(n-1)$, which we treat in some detail in order to summarize well-known facts about simple Lie algebras. Facts valid for arbitrary simple Lie algebras will be given under the heading of "Property," and their proofs will not be given here since they are readily available in the literature [6, 9]. We shall reserve the title of "Theorem" for properties directly related to partitions. The forms used here for the roots and weights of $A(n-1)$ will be derived, whereas in the following sections their forms for $B(n)$, $C(n)$, and $D(n)$ will be written down without derivations; all the forms for the roots and weights used here are given in [6].

We shall use a realization of the (n^2-1)-dimensional Lie algebra $A(n-1)$ in terms of $n \times n$ matrices, choosing as its basis the traceless diagonal matrices h_i, $i = 1, \ldots, n$, where h_i has $(n-1)/n$ as its (i, i)th element and $-1/n$ for its other diagonal elements, and the $e_{jk}, j \neq k = 1, \ldots, n$, where e_{jk} has 1 for its (j, k)th element and 0 for its other elements. The h_i, which span the Cartan subalgebra of $A(n-1)$, satisfy the relation $h_1 + \cdots + h_n = 0$, so only $n-1$ of them are linearly independent. We find it convenient to use the above linearly dependent set as opposed to a linearly independent subset since they give rise to extremely simple forms for the roots. These forms will turn out to be n-tuples, like the forms for the roots of the other Lie algebras, and it is for this reason that we consider $A(n-1)$ rather than $A(n)$.

The commutation relations of the h_i, e_{jk} are

$$[h_i, h_j] = 0, \qquad i, j = 1, \ldots, n, \tag{11}$$

$$[h_i, e_{jk}] = (\delta_{ij} - \delta_{ik})e_{jk}, \qquad i = 1, \ldots, n, \quad j \neq k = 1, \ldots, n, \tag{12}$$

and

$$[e_{jk}, e_{lm}] = \begin{cases} h_j - h_k, & l = k, \quad m = j \\ e_{jm}, & l = k, \quad m \neq j \\ -e_{lk}, & l \neq k, \quad m = j \\ 0, & l \neq k, \quad m \neq j. \end{cases} \tag{13}$$

Using the shorthand notation $\mathbf{h} \equiv (h_1, \ldots, h_n)$, we may write (12) as

$$[\mathbf{h}, e_{jk}] = \alpha_{jk} e_{jk} \tag{14}$$

and the first of Eqs. (13) as

$$[e_{jk}, e_{kj}] = \alpha_{jk} \cdot \mathbf{h} \tag{15}$$

where

$$\alpha_{jk} = (\overset{1}{0}, \ldots, 0, \overset{j}{1}, 0, \ldots, 0, \overset{k}{-1}, 0, \ldots, \overset{n}{0}) \equiv (\overset{j}{1}, \overset{k}{-1}). \tag{16}$$

The $n(n-1)$ n-tuples α_{jk} are the roots of $A(n-1)$. Clearly $\alpha_{kj} = -\alpha_{jk}$ and $\alpha_{jk} \cdot \alpha_{jk} = 2$; they also lie on the $(n-1)$-dimensional hyperplane

$$x_1 + \cdots + x_n = 0,$$

so only $n-1$ of them are linearly independent. We shall choose a basis for this hyperplane shortly.

Definition 1 (a) A real nonzero n-tuple $\mathbf{L}$ is called "positive" if its first nonzero component, reading from left to right, is positive; otherwise it is called "negative."

(b) If $\mathbf{L}$ and $\mathbf{L}'$ are two real n-tuples, $\mathbf{L}$ is said to be "higher" than $\mathbf{L}'$ if the n-tuple $\mathbf{L} - \mathbf{L}'$ is positive. It is easy to see that α_{jk} is a positive root if $j < k$, and that if α_{jk} and α_{lm} are positive, α_{jk} is higher than α_{lm} if either $j < l$, or $j = l$ and $m < k$.

Definition 2 A positive root is called "simple" if it cannot be expressed as the sum of two positive roots.

Property 1 The simple roots of a simple Lie algebra form a basis for the Lie algebra's root space, the other roots being linear combinations with integral coefficients of the simple roots.

Definition 3 The number of simple roots is called the "rank" of the Lie algebra.

$A(n-1)$ has rank $n-1$, its simple roots being $\alpha_i \equiv \alpha_{i,i+1}$, $i = 1, \ldots, n-1$, as can easily be verified. An arbitrary positive root α_{jk} is given in terms of them by

$$\alpha_{jk} = \sum_{i=j}^{k-1} \alpha_i . \tag{17}$$

Definition 4 The group generated by the reflections in hyperplanes perpendicular to the roots of a simple Lie algebra is called the "Weyl group" of the Lie algebra.

Property 2 The Weyl group leaves the set of roots of a simple Lie algebra invariant.

Let $\mathbf{L} = (l_1, \ldots, l_n)$, and $S_{jk}\mathbf{L}$ be the n-tuple obtained from $\mathbf{L}$ by reflecting it in the hyperplane perpendicular to α_{jk}, so

$$S_{jk}\mathbf{L} = \mathbf{L} - \frac{2(\alpha_{jk} \cdot \mathbf{L})}{(\alpha_{jk} \cdot \alpha_{jk})}\alpha_{jk} = \mathbf{L} - (\alpha_{jk} \cdot \mathbf{L})\alpha_{jk} . \tag{18}$$

Using Eq. (16) for α_{jk}, we obtain

$$S_{jk}\mathbf{L} = (l_1, \ldots, \overset{j}{l_k}, \ldots, \overset{k}{l_j}, \ldots, l_n),$$

so S_{jk} just permutes the jth and kth components of $\mathbf{L}$. The Weyl group for $A(n-1)$ therefore consists of all permutations of the components of $\mathbf{L}$ and so is isomorphic to the symmetric group $S(n)$. This clearly leaves invariant the set of roots of $A(n-1)$, and in fact any two roots may be connected by at most two reflections: $\alpha_{lm} = S_{jl}S_{mk}\alpha_{jk}$.

We now consider the classification of irreducible representations of $A(n-1)$: Let D be an N-dimensional irreducible representation of $A(n-1)$ with representatives

$$D(h_i) \equiv H_i , \qquad D(e_{jk}) \equiv E_{jk}$$

satisfying the hermiticity conditions

$$H_i^\dagger = H_i , \qquad E_{jk}^\dagger = E_{kj} . \tag{19}$$

These are precisely the conditions required in order that the exponential map of D yields a unitary representation of the unimodular unitary group $SU(n)$.

We denote the carrier space for D by R and choose its basis to consist of simultaneous eigenvectors of the H_i:

$$H_i\psi_p = \mu_{ip}\psi_p , \qquad i = 1, \ldots, n, \quad p = 1, \ldots, N.$$

Denoting $\mathbf{M}_p \equiv (\mu_{1p}, \ldots, \mu_{np})$, this equation may be written in the compact form

$$\mathbf{H}\psi_p = \mathbf{M}_p\psi_p, \qquad p = 1, \ldots, N. \tag{20}$$

$\mathbf{M}_p$ is called a "weight" of the representation D; we denote the set of all weights of D by $W(D)$. Because of the hermiticity of the H_i (with respect to some inner product on R), elements of $W(D)$ are real n-tuples; furthermore, from $H_1 + \cdots + H_n = 0$, we obtain $\mu_{1p} + \cdots + \mu_{np} = 0$, $p = 1, \ldots, N$, so elements of $W(D)$ belong to the root hyperplane.

Definition 5 The "multiplicity" of a weight $\Lambda \in W(D)$, denoted γ_Λ, is the number of linearly independent corresponding basis vectors $\in R$.

Definition 6 A weight Λ is "simple" if $\gamma_\Lambda = 1$.

We employ the same method of ordering weights as we did for arbitrary n-tuples, and thereby allow consideration of the highest weight of an irreducible representation D.

Property 3 The highest weight of an irreducible representation of a simple Lie algebra is simple; and if two irreducible representations have the same highest weight, they are equivalent.

The problem of classifying irreducible representations of a simple Lie algebra is therefore equivalent to the problem of classifying its highest weights.

Property 4 Any two weights $\in W(D)$ differ by an integral linear combination of the roots and therefore also, by Property 1, by an integral linear combination of the simple roots.

In particular, therefore, given the highest weight Λ of $W(D)$, any other weight $\in W(D)$ may be obtained by a suitable subtraction of simple roots from Λ.

Property 5 If $\mathbf{M} \in W(D)$ and α is a root of the Lie algebra, then $2(\alpha \cdot \mathbf{M})/(\alpha \cdot \alpha)$ is an integer, and $S_\beta\mathbf{M} \equiv \mathbf{M} - (2(\alpha \cdot \mathbf{M})/(\alpha \cdot \alpha))\alpha \in W(D)$. This implies that $W(D)$ is invariant under the action of elements of the Weyl group.

Definition 7 Two weights are called "equivalent" if they can be obtained from each other by an element of the Weyl group. The set of all weights equivalent to a given weight is called a "shell" of $W(D)$.

For $A(n-1)$, therefore, the shell containing a weight $\mathbf{M}$ consists of all n-tuples obtained by permuting the components of $\mathbf{M}$.

Property 6 If p is an integer such that $0 \leq p \leq (\boldsymbol{\alpha} \cdot \mathbf{M})/(\boldsymbol{\alpha} \cdot \boldsymbol{\alpha})$, then:

(a) $\gamma(\mathbf{M} - p\boldsymbol{\alpha}) = \gamma(S_{\alpha}\mathbf{M} + p\boldsymbol{\alpha})$;
(b) $\gamma(\mathbf{M} - p\boldsymbol{\alpha}) \geq \gamma(\mathbf{M} - (p-1)\boldsymbol{\alpha})$.

This property implies that a chain of weights, $\mathbf{M}$, $\mathbf{M} - \boldsymbol{\alpha}, \ldots,$ $\mathbf{M} - (2(\boldsymbol{\alpha} \cdot \mathbf{M})/(\boldsymbol{\alpha} \cdot \boldsymbol{\alpha}))\boldsymbol{\alpha}$, is spindle shaped, and in particular that equivalent weights have the same multiplicity.

Definition 8 The highest weight in a shell is called a "dominant weight." Clearly the highest weight $\boldsymbol{\Lambda}$ is itself a dominant weight.

For the case of $A(n-1)$, let $\mathbf{M} \equiv (\mu_1, \ldots, \mu_n)$ be a dominant weight, and suppose $\mu_j < \mu_k$ for some $j < k$. Then

$$S_{jk}\mathbf{M} - \mathbf{M} = (\ldots, \overset{j}{\mu_k}, \ldots, \overset{k}{\mu_j}, \ldots) - (\ldots, \overset{j}{\mu_j}, \ldots, \overset{k}{\mu_k}, \ldots)$$
$$= (0, \ldots, 0, \overset{j}{\mu_k - \mu_j}, 0, \ldots, 0, \overset{k}{\mu_j - \mu_k}, 0, \ldots, 0)$$

which is clearly positive; since $S_{jk}\mathbf{M}$ is equivalent to $\mathbf{M}$, this contradicts the assumption that $\mathbf{M}$ is a dominant weight. Hence if $\mathbf{M}$ is a dominant weight, its components satisfy the inequalities $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n$.

Now let $\mathbf{M}$ be an arbitrary weight $\in W(D)$; by Property 5 applied to $A(n-1)$, $\mathbf{M} \cdot \boldsymbol{\alpha}_{jk}$ is an integer for all $\boldsymbol{\alpha}_{jk}$, so $\mu_j - \mu_k$ is an integer for all $j, k = 1, \ldots, n$. This means that all components of $\mathbf{M}$ have the same fractional part, and also, by Property 4, that the components of all weights $\in W(D)$ have the same fractional part.

The next property, due to Freudenthal [9], enables one to calculate the multiplicity of an arbitrary weight.

Property 7 Let $\boldsymbol{\alpha}$ be a positive root of a simple Lie algebra, $\boldsymbol{\delta}$ half the sum of all the positive roots, and $\boldsymbol{\Lambda}$ and $\mathbf{M}$ the highest weight and an arbitrary weight, respectively, of $W(D)$. Then

$$\gamma(\mathbf{M}) - \frac{2\sum_{\alpha>0}\sum_{k=1}^{\infty}\gamma(\mathbf{M}+k\boldsymbol{\alpha})((\mathbf{M}+k\boldsymbol{\alpha})\cdot\boldsymbol{\alpha})}{(\boldsymbol{\Lambda}+\boldsymbol{\delta})\cdot(\boldsymbol{\Lambda}+\boldsymbol{\delta}) - (\mathbf{M}+\boldsymbol{\delta})\cdot(\mathbf{M}+\boldsymbol{\delta})} \tag{21}$$

where $\gamma(\mathbf{M} + k\boldsymbol{\alpha}) \equiv 0$ if $\mathbf{M} + k\boldsymbol{\alpha} \notin W(D)$.

We now consider the classification of highest weights $\boldsymbol{\Lambda}$ of a simple Lie algebra, denoting the irreducible representations corresponding to $\boldsymbol{\Lambda}$ by $D(\boldsymbol{\Lambda})$, and $W(D(\boldsymbol{\Lambda}))$ by $W(\boldsymbol{\Lambda})$. Now since $\boldsymbol{\Lambda}$ lies in the root hyperplane, it is uniquely determined by the numbers $g_i \equiv 2\boldsymbol{\Lambda} \cdot \boldsymbol{\alpha}_i/\boldsymbol{\alpha}_i \cdot \boldsymbol{\alpha}_i$, where $\boldsymbol{\alpha}_i$ are the simple roots. Due to Property 5 and the fact that $\boldsymbol{\Lambda}$ is a highest weight, these are all nonnegative integers. The numbers g_i themselves therefore give a unique label for the irreducible representations. For $A(n-1)$ it is easy to

show that if $\Lambda = (\lambda_1, \ldots, \lambda_n)$ is the highest weight of an irreducible representation, then $g_i = (\lambda_i - \lambda_{i+1})$, $i = 1, \ldots, n-1$.

Definition 9 A nonzero highest weight that cannot be expressed as the sum of two nonzero highest weights is called a "fundamental" highest weight, and the corresponding representation a "fundamental" representation.

Property 8 The fundamental highest weights are Λ^i, for which $g_j = \delta_{ij}$. There are therefore as many fundamental highest weights as there are simple roots and can therefore also be chosen as a basis for the root or weight space; in fact if Λ is any highest weight, then $\Lambda = \sum_i g_i \Lambda^i$.

For $A(n-1)$ there are $n-1$ fundamental weights and corresponding representations; suppose $\Lambda^i = (\lambda_1, \ldots, \lambda_n)$, then since $\Lambda^i \cdot \alpha_j = \delta_{ij}$ we have $\lambda_1 = \cdots = \lambda_i = \lambda_{i+1} + 1 = \cdots = \lambda_n + 1$, and since Λ^i lies in the root hyperplane $\lambda_1 + \cdots + \lambda_n = 0$. Solving for λ_1 gives $\lambda_1 = (n-i)/n$, so

$$\Lambda^i = \left(\overset{1}{\frac{n-i}{n}}, \ldots, \overset{i}{\frac{n-i}{n}}, \overset{i+1}{\frac{-i}{n}}, \ldots, \overset{n}{\frac{-i}{n}}\right).$$

Let $N(\Lambda)$ be the dimension of $D(\Lambda)$; now since the simple roots are a basis for the root space, we may write

$$\Lambda = \sum_i l_i \alpha_i \tag{22}$$

where the sum extends over all simple roots ($i = 1, \ldots, n-1$ for $A(n-1)$ and $i = 1, \ldots, n$ for the other simple Lie algebras). In general, of course, the l_i will differ from the g_i above. Also, an arbitrary weight $\mathbf{M} \in W(\Lambda)$ may be written

$$\mathbf{M} = \sum_i m_i \alpha_i , \tag{23}$$

so

$$\Lambda - \mathbf{M} = \sum_i (l_i - m_i)\alpha_i ,$$

which simply expresses the fact that $\mathbf{M}$ may be obtained from Λ by the subtraction of a suitable number of simple roots. Clearly, then, $l_i - m_i$ must be a nonnegative integer. Let

$$\mu(\Lambda, \mathbf{M}) = \sum_i (l_i - m_i), \tag{24}$$

so $\mu(\Lambda, \mathbf{M})$ is the total number of subtractions of simple roots needed to give $\mathbf{M}$ from Λ. Let Λ' be the lowest weight $\in W(\Lambda)$; if $\Lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$, then for $A(n-1)$ clearly $\Lambda' = (\lambda_n, \ldots, \lambda_2, \lambda_1)$.

Definition 10 The "height" $T(\Lambda)$ of $D(\Lambda)$ is defined by $T(\Lambda) = \mu(\Lambda, \Lambda')$.

Definition 11 A "layer" of $W(\Lambda)$ is a subset $\omega_j(\Lambda)$ consisting of all $\mathbf{M} \in W(\Lambda)$ such that $\mu(\Lambda, \mathbf{M}) = j$.

$\omega_j(\Lambda)$ therefore consists of all $\mathbf{M}$ obtainable from Λ by the subtraction of j (not necessarily distinct) simple roots. Clearly the number of layers of $W(\Lambda) = T(\Lambda) + 1$ and $W(\Lambda) = \bigcup_{j=0}^{T(\Lambda)} \omega_j(\Lambda)$.

Let $s_j(\Lambda)$ denote the number of weights $\in \omega_j(\Lambda)$, in which each weight is counted a number of times equal to its multiplicity. Then $N(\Lambda) = \sum_{j=0}^{T(\Lambda)} s_j(\Lambda)$, and because of the simplicity of Λ and Λ', we have $s_0(\Lambda) = s_{T(\Lambda)}(\Lambda) = 1$.

Property 9 The layers of $W(\Lambda)$ are spindle shaped, i.e., $s_j(\Lambda) = s_{T(\Lambda)-j}(\Lambda)$ and $s_0(\Lambda) \leq s_1(\Lambda) \leq \cdots \leq s_r(\Lambda)$ where $r = [\frac{1}{2}T(\Lambda)]$ (the largest integer $\leq \frac{1}{2}T(\Lambda)$).

It is this property that we shall apply to the fundamental representations to derive our theorems on various types of partitions of integers.

We now consider the case of $A(n-1)$ and show that $s_j(\Lambda^i)$ equals the partition $(j; n-i, i)$ of j into at most $n-i$ positive integers none of which exceeds i. Now

$$\Lambda^i = (\overset{1}{a}, \ldots, \overset{i}{a}, \overset{i+1}{a-1}, \ldots, \overset{n}{a-1}) \qquad \text{where} \quad a = (n-i)/n,$$

and the only simple root that may be subtracted from it is α_i, and this may be subtracted only once to give

$$\Lambda^i - \alpha_i = (\overset{1}{a}, \ldots, \overset{i-1}{a}, \overset{i}{a-1}, \overset{i+1}{a}, \overset{i+2}{a-1}, \ldots, \overset{n}{a-1})$$

which is equivalent to Λ^i. Next, the only simple roots that one may subtract (again just once) from $\Lambda^i - \alpha_i$ are $\alpha_{i\pm 1}$, again to yield weights equivalent to Λ^i. Repeating this process it is easy to see that if $\mathbf{M} \in W(\Lambda^i)$, the only permissible subtraction of a simple root from it is one which interchanges an $a-1$ with an a immediately preceding it, this being achieved by a single subtraction. This shows that every weight $\in W(\Lambda^i)$ is equivalent to Λ^i, and therefore simple. The dimension of $D(\Lambda^i)$ therefore equals the number of distinct permutations of the components of Λ^i, and this equals the number of ways of choosing i components to be a, i.e.,

$$N(\Lambda^i) = \binom{n}{i}. \tag{25}$$

Next, $T(\Lambda^i)$ equals the number of subtractions of a simple root from Λ^i to obtain the lowest weight

$$\Lambda'^i = (\overset{1}{a-1}, \ldots, \overset{n-i}{a-1}, \overset{n-i+1}{a}, \ldots, \overset{n}{a}).$$

Clearly, Λ'^i is obtained from Λ^i by i interchanges of the first $a-1$ (reading from the left) with the preceding a, followed by i similar interchanges of the second $a-1$, and so on. Each step in the process involves the subtraction of a single simple root, so since there are $n-i$ $(a-1)$'s, we have

$$T(\Lambda^i) = i(n-i). \tag{26}$$

Finally, we calculate $s_j(\Lambda^i)$; since each weight of $W(\Lambda^i)$ is simple, this equals the number of weights $\in \omega_j(\Lambda^i)$. We must therefore calculate the number of distinct ways of subtracting j simple roots from Λ^i, in other words the number of distinct ways of successively interchanging j $(a-1)$'s with preceding a's. Suppose, for $l = 1, \ldots, n-i$, the lth $a-1$ undergoes k_l such successive interchanges; clearly the $(l+1)$th $a-1$ cannot have more such interchanges than the lth $a-1$, and since there are i a's, no $a-1$ may undergo more than i interchanges. $s_j(\Lambda^i)$ is therefore the number of distinct solutions of the equation $k_1 + \cdots + k_{n-i} = j$ subject to the conditions $k_1 \geq k_2 \geq \cdots \geq k_{n-i}$ and $k_l \leq i$ for $l = 1, \ldots, n-1$. But this is just the partition function $(j; n-i, i)$; hence

$$s_j(\Lambda^i) = (j; n-i, i). \tag{27}$$

Equations (25) and (26) and Property 9 now imply the following properties of $(j; n-i, i)$:

$$\sum_{j=0}^{i(n-i)} (j; n-i, i) = \binom{n}{i},$$

which is just the Eq. (4) trivially derived using generating functions in Section 1, and

Theorem 1

(a) $(j; n-i, i) = (i(n-i) - j; n-i, i)$;

(b) $(j; n-i, i) \geq (j-1, n-i, i)$ for $0 \leq j \leq [i(n-i)/2]$.

Theorem 1a is, as mentioned in Section 1, merely a statement of the reciprocal nature of the Gaussian polynomial $\begin{bmatrix} n \\ i \end{bmatrix}(q)$. Theorem 1b, on the other hand, is not trivial and although it was in fact proved a long time ago by Elliott [5] using invariant theory of quantics; it does not appear to be very widely known.

3. $B(n)$

Having in the preceding section given the general method for deriving the simple roots and fundamental weights of a Lie algebra, we shall content ourselves in this and the following sections with writing them down without derivation (these can all be found in [6]). $B(n)$ is the Lie algebra of the group,

$O(2n+1)$ of $(2n+1) \times (2n+1)$ orthogonal matrices, and has rank n. Its positive roots are n-tuples of the form

$$(0, \ldots, 0, \overset{j}{1}, 0, \ldots, 0 \pm \overset{k}{1}, 0, \ldots, 0) \quad \text{and} \quad (0, \ldots, 0, \overset{i}{1}, 0, \ldots, 0),$$

the simple roots being

$$\alpha_i = (0, \ldots, 0, \overset{i}{1}, \overset{i+1}{-1}, 0, \ldots, 0) \quad \text{for} \quad i = 1, \ldots, n-1,$$

and $\alpha_n = (0, \ldots, 0, 1)$, so $2(\alpha_i \cdot \mathbf{L})/(\alpha_i \cdot \alpha_i) = \alpha_i \cdot \mathbf{L}$, $i = 1, \ldots, n-1$, and $2(\alpha_n \cdot \mathbf{L})/(\alpha_n \cdot \alpha_n) = 2(\alpha_n \cdot \mathbf{L})$. Using $2(\Lambda^i \cdot \alpha_j)/(\alpha_j \cdot \alpha_j) = \delta_{ij}$, we find the fundamental highest weights to be

$$\Lambda^i = (\overset{1}{1}, \ldots, \overset{i}{1}, \overset{i+1}{0}, \ldots, \overset{n}{0}), \quad i = 1, \ldots, n-1, \quad \text{and} \quad \Lambda^n = (\tfrac{1}{2}, \ldots, \tfrac{1}{2}).$$

We treat the nth fundamental representation separately from the rest, dealing with it first.

By Property 5, the only simple root that may be subtracted from Λ^n is α_n, this being subtractible only once to give $\Lambda^n - \alpha_n = (\frac{1}{2}, \ldots, \frac{1}{2}, -\frac{1}{2})$, which is equivalent to Λ^n. α_{n-1} may be subtracted once from this to give the weight $(\frac{1}{2}, \ldots, \frac{1}{2}, -\frac{1}{2}, \frac{1}{2})$, and from this, one may either subtract α_{n-2} to give $(\frac{1}{2}, \ldots, \frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{1}{2})$, or α_n again to give $(\frac{1}{2}, \ldots, \frac{1}{2}, -\frac{1}{2}, -\frac{1}{2})$. It is easy to see, in fact, that an arbitrary weight $\mathbf{M} \in W(\Lambda^n)$ has either $\frac{1}{2}$ or $-\frac{1}{2}$ for its components, a subtraction of a simple root being equivalent to either interchanging a $-\frac{1}{2}$ with an immediately preceding $\frac{1}{2}$ or to changing an nth $\frac{1}{2}$ into a $-\frac{1}{2}$. At no stage can a simple root be subtracted more than once, so each weight is equivalent to Λ^n and therefore simple. Clearly, the lowest weight is $\Lambda'^n = (-\frac{1}{2}, \ldots, -\frac{1}{2})$.

Now the number of weights with l $-\frac{1}{2}$'s is $\binom{n}{l}$, so the dimension of $D(\Lambda^n)$ is given by

$$N(\Lambda^n) = \sum_{l=0}^{n} \binom{n}{l} = 2^n. \tag{28}$$

Also, in order to obtain Λ'^n from Λ^n one must change the nth $\frac{1}{2}$ into a $-\frac{1}{2}$ and then permute it step by step with the immediately preceding $\frac{1}{2}$ until one obtains, after n simple subtractions, $(-\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2})$. Repeating the process for this weight one obtains, after a further $n-1$ simple subtractions, $(-\frac{1}{2}, -\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2})$ and so on. By the time Λ'^n is attained, the total number of simple subtractions undergone is $n + (n-1) + \cdots + 2 + 1$, so

$$T(\Lambda^n) = \tfrac{1}{2}n(n+1). \tag{29}$$

Next, $s_j(\Lambda^n)$ is the number of distinct ways of subtracting j simple roots from Λ^n; suppose, for some $\mathbf{M} \in \omega_j(\Lambda^n)$, the lth $-\frac{1}{2}$ is in the $(n - k_l + 1)$th position, where the $-\frac{1}{2}$'s are numbered from the left and we interpret a $-\frac{1}{2}$ in the $(n+1)$th position as a $\frac{1}{2}$ in the nth position. The replacement of a $\frac{1}{2}$ in

this position by the $-\frac{1}{2}$ is achieved by k_l simple subtractions. Clearly, no k_l can exceed n, and $k_l > k_{l+1}$ unless they are both zero; therefore $j = k_1 + \cdots + k_n$, and

$$s_j(\Lambda^n) = P(j; n, n), \tag{30}$$

where $P(j; n, n)$ is the number of partitions of j into at most n strictly decreasing integers, none of which exceeds n.

Equations (29) and (30) now imply that

$$\sum_{j=0}^{n(n+1)/2} P(j; n, n) = 2^n$$

which is just Eq. (6) derived using the generating function of $P(j; n, n)$; and Property 9 implies:

Theorem 2

(a) $P(j; n, n) = P(\frac{1}{2}n(n+1) - j; n, n)$;
(b) $P(j; n, n) \geq P(j-1; n, n)$ for $j \leq [\frac{1}{4}n(n+1)]$.

(a) is, again, merely a statement of the reciprocal nature of the generating function for $P(j; n, n)$; (b) appears to be new.

We now consider the general case of Λ^i, $i \neq n$. By the subtraction of simple roots α_i, $i \neq n$, we obtain all weights whose components are permutations of those of Λ^i, and so which have i components equal to 1 and $n - i$ components equal to zero. These weights are all equivalent to Λ^i since at any given time a given α_i may be subtracted only once. For any such weight with 1 for its nth component we may also subtract α_n either once to give a weight with 0 for its nth component, or twice to give a weight with -1 for its nth component. The latter weight is equivalent to the original weight and therefore also to Λ^i, whereas the former weight is not.

Proceeding in this manner we see that $W(\Lambda^i)$ consists of all weights with a number $\leq i$ of components equal to ± 1, the rest of the components being zero. For any such weight α_i may be subtracted once if the ith component is 1 and the $(i+1)$th component is zero or if the ith component is zero and the $(i+1)$th component is -1, but if the ith component is 1 and the $(i+1)$th component is -1, α_i may be subtracted either once to give a weight with two more zero components or twice to give a weight with the 1 and -1 interchanged. If the nth component is 1, α_n may be subtracted either once to give a weight with one more zero component or twice to give a weight with the nth component equal to -1. Weights with the same number of ± 1's are equivalent and so belong to the same shell. Let G_k denote the shell consisting of weights with $i - k$ components equal to ± 1 and $n - i + k$ zero components; clearly

$$W(\Lambda^i) = \bigcup_{k=0}^{i} G_k . \tag{31}$$

The lowest weight

$$\Lambda'^{i} = (\overset{1}{-1}, \ldots, \overset{i}{-1}, 0, \ldots, \overset{n}{0}) \in G_0,$$

and the dominant weight of G_k is

$$\mathbf{M}_k = (\overset{1}{1}, \ldots, \overset{i-k}{1}, 0, \ldots, \overset{n}{0}).$$

We use $\mathbf{M}_k$ to calculate the multiplicity of weights $\in G_k$, using Freudenthal's formula, Eq. (21), and denoting $\gamma(\mathbf{M}_k)$ by N_k for short. First, using $\boldsymbol{\delta} = \frac{1}{2}(2n-1, 2n-3, \ldots, 3, 1)$ we obtain $(\boldsymbol{\Lambda}^i + \boldsymbol{\delta}) \cdot (\boldsymbol{\Lambda}^i + \boldsymbol{\delta}) - (\mathbf{M}_k + \boldsymbol{\delta}) \cdot (\mathbf{M}_k + \boldsymbol{\delta}) = k(2n - 2i + k + 1)$. Secondly, $n - i + k$ positive roots of the type $(0, \ldots, 0, 1, 0, \ldots, 0)$ may be added to $\mathbf{M}_k$ once only to give a weight of G_{k-1}, whereas $(n - i + k)(n - i + k - 1)$ positive roots of the type $(0, \ldots, 0, 1, 0, \ldots, 0, \pm 1, 0, \ldots, 0)$ may be added once only to give a weight of G_{k-2}. In each such case, $(\mathbf{M}_k + \boldsymbol{\alpha}) \cdot \boldsymbol{\alpha} = (\boldsymbol{\alpha} \cdot \boldsymbol{\alpha})$, so substituting into Eq. (21) we obtain the recursion relation

$$k(2n - 2i + k + 1)N_k = 2(n - i + k)(2(n - i + k - 1)N_{k-2} + N_{k-1}), \qquad k \geq 1,$$

where $N_{-1} = 0$. Using $N_0 = 1$ we obtain easily $N_1 = 1$; the solution of the recursion relation subject to these conditions is

$$N_{2k} = \binom{n - i + 2k}{k}, \qquad N_{2k+1} = \binom{n - i + 2k + 1}{k}. \tag{32}$$

Consider G_k; weights in this shell have $(n - i + k)$ zero components which may be in any of $\binom{n}{i-k}$ distinct arrangements. For any one of these arrangements, suppose there are j 1's and $(i - k - y)$ -1's; there are $\binom{i-k}{j}$ such arrangements of the ± 1's, so the total number of weights with $(n - i + k)$ 0's in any given arrangement is

$$\sum_{j=0}^{i-k} \binom{i-k}{j} = 2^{i-k}.$$

Hence the number of distinct weights in G_k is $\binom{n}{i-k}2^{i-k}$ and the multiplicity of G_k is $N_k\binom{n}{i-k}2^{i-k}$. Summing over all shells we obtain the dimension of $D(\boldsymbol{\Lambda}^i)$; this is given in Table 30 of [6] as $\binom{2n+1}{i}$, which is therefore the value of the above sum:

$$N(\boldsymbol{\Lambda}^i) = \sum_{k=0}^{i} N_k \binom{n}{i-k} 2^{i-k} = \binom{2n+1}{i}, \qquad i = 1, \ldots, n-1. \tag{33}$$

We next calculate the height of $W(\boldsymbol{\Lambda}^i)$; let

$$\boldsymbol{\Lambda}^i_j = (-1, \ldots, \overset{j}{-1}, 1, \ldots, \overset{i}{1}, 0, \ldots, 0)$$

so that $\Lambda^i \equiv \Lambda_0^i$, $\Lambda'^i = \Lambda_i^i$; now

$$\Lambda_j^i = \Lambda_{j-1}^i - 2(0, \ldots, 0, \overset{j}{1}, 0, \ldots, 0) = \Lambda_{j-1}^i - 2(\alpha_j + \cdots + \alpha_n),$$

so Λ_j^i is $2(n-j+1)$ layers down from Λ_{j-1}^i. Hence Λ_i^i is $2(n + (n-1) + \cdots + (n-i+1))$ layers down from Λ_0^i, i.e.,

$$T(\Lambda^i) = i(2n - i + 1). \tag{34}$$

We now consider an arbitrary weight of G_k and determine to which layer it belongs by calculating how many layers down it is from $\mathbf{M}_k$. $\mathbf{M}_k$ itself can easily be shown, in a manner analogous to that used to calculate $T(\Lambda^i)$, to belong to $\omega_{k(2n-2i+k+1)/2}(\Lambda^i)$. Let $\mathbf{M}_k(l_1, \ldots, l_{i-k})$ be the weight $\in G_k$ with $i-k$ 1's in which, for $\lambda = 1, \ldots, i-k$, the λth 1 is, reading from the left, in the l_λth position (so $1 \leq l_1 < l_2 < \cdots < l_{i-k} \leq n$). To get to this weight from $\mathbf{M}_k$, the λth 1 must be moved forward $l_\lambda - \lambda$ places, each such movement by one place being achieved by a single subtraction of a simple root. $\mathbf{M}_k(l_1, \ldots, l_{i-k})$ is therefore

$$\sum_{\lambda=1}^{i-k} (l_\lambda - \lambda) = \sum_{\lambda=1}^{i-k} l_\lambda - \tfrac{1}{2}(i-k)(i-k+1)$$

layers down from $\mathbf{M}_k$.

Next, let $\mathbf{M}_{k(l_1, \ldots, l_{i-k})}^{h(m_1, \ldots, m_h)}$ be the weight with $(i-k) \pm 1$'s of which h $(0 \leq h \leq i-k)$ are -1's such that the 0's are in the same position as in $\mathbf{M}_k(l_1, \ldots, l_{i-k})$, and such that, for $\mu = 1, \ldots, h$, the μth -1 is in the l_{m_μ}th position, where $1 \leq m_1 < m_2 < \cdots < m_h \leq i-k$. Now since it takes $2(n - l_{m_\mu} + 1)$ simple subtractions to replace 1 in the l_{m_μ}th position by a -1, to get from $\mathbf{M}_k(l_1, \ldots, l_{i-k})$ to $\mathbf{M}_{k(l_1, \ldots, l_{i-k})}^{h(m_1, \ldots, m_h)}$ requires

$$2\sum_{\mu=1}^{h} (n - l_{m_\mu} + 1) = 2h(n+1) - 2\sum_{\mu=1}^{h} l_{m_\mu}$$

simple subtractions. The number of simple subtractions needed to get from $\mathbf{M}_k$ to $\mathbf{M}_{k(l_1, \ldots, l_{i-k})}^{h(m_1, \ldots, m_h)}$ is therefore

$$\sum_{\lambda=1}^{i-k} l_\lambda - 2\sum_{\mu=1}^{h} l_{m_\mu} - \tfrac{1}{2}(i-k)(i-k+1) + 2h(n+1)$$

$$= \sum_{\lambda=1}^{i-k} \delta_\lambda^h l_\lambda - \tfrac{1}{2}(i-k)(i-k+1) + 2h(n+1)$$

where h of the δ_λ^h are -1 and the rest are $+1$. Finally, therefore, $\mathbf{M}_{k(l_1, \ldots, l_{i-k})}^{h(m_1, \ldots, m_h)}$ is on ω_j, where

$$j = \sum_{\lambda=1}^{i-k} \delta_\lambda^h l_\lambda + (n+1)(2h+k) - \tfrac{1}{2}i(i+1).$$

Let $Q(j'; a, b, c)$ be the number of partitions of j' into exactly a strictly increasing positive integers none of which exceeds b and in which c of the integers contribute negatively. From the above it is easy to see that

$$S_j(\Lambda^i) = \sum_{k=0}^{i} N_k \sum_{h=0}^{i-k} Q(j - (n+1)(2h+k) + \tfrac{1}{2}i(i+1); i-k, n, h). \quad (35)$$

Using Eq. (34) we see that

$$\sum_{j=0}^{i(2n-i+1)} \sum_{h=0}^{i-k} Q(j - (n+1)(2h+k) + \tfrac{1}{2}i(i+1); i-k, n, h)$$

is the number of distinct weights $\in G_k$. We have already seen that this number is $\binom{n}{i-k}2^{i-k}$, and the equality of these two expressions can easily be shown using Eq. (8), with the appropriate values for j', a, b, and c ($j'_{\min}$ and $j'_{\max}$ are easily seen to correspond to $j = 0$ and $j = i(2n-i+1)$, respectively). Clearly, Eq. (10) could have been used to derive the formula for the number of distinct weights of G_k, but no great advantage would have ensued from doing so.

Property 9 of the last section shows the following to hold:

Theorem 3 *For* $i = 1, \ldots, n-1$,

(a) $$\sum_{k=0}^{i} N_k \sum_{h=0}^{i-k} Q(j - (n+1)(2h+k) + \tfrac{1}{2}i(i+1); i-k, n, h)$$

$$= \sum_{k=0}^{i} N_k \sum_{h=0}^{i-k} Q(i(2n-i+1) - j - (n+1)(2h+k) + \tfrac{1}{2}i(i+1); i-k, n, h).$$

(b) $$\sum_{k=0}^{i} N_k \sum_{h=0}^{i-k} \left| \begin{matrix} Q(j - (n+1)(2h+k) + \tfrac{1}{2}i(i+1); i-k, n, h) \\ -Q(j-1 - (n+1)(2h+k) + \tfrac{1}{2}i(i+1); i-k, n, h) \end{matrix} \right| \geq 0$$

for $0 \leq j \leq \tfrac{1}{2}i(2n-i+1)$.

As mentioned in Section 1, (a) follows easily from the property $Q(j'; a, b, c) = Q(-j'; a, b, a-c)$ when the appropriate values of j', a, b, and c are taken, and in fact the equation holds with the $\sum_{k=0}^{i} N_k$ omitted so that the shells themselves have a symmetric layer structure. This is a fact that does not follow from Dynkin's theorem; the author does not know whether it is generally known. No previous proof of (b) appears to have been given.

4. $C(n)$

$C(n)$ is the Lie algebra of the group $S_p(2n)$ of symplectic matrices of order $2n$, and again has rank n. Its positive roots are again n-tuples of the form

$$(0, \ldots, 0, \overset{j}{1}, 0, \ldots, 0, \overset{k}{\pm 1}, 0, \ldots, 0)$$

(like $B(n)$) and (unlike $B(n)$)

$$(0, \ldots, 0, \overset{i}{2}, 0, \ldots, 0),$$

the simple roots being

$$\alpha_i = (0, \ldots, 0, \overset{i}{1}, \overset{i+1}{-1}, 0, \ldots, 0) \qquad \text{and} \qquad \alpha_n = (0, \ldots, 0, 2);$$

here $2(\alpha_n \cdot \mathbf{L})/(\alpha_n \cdot \alpha_n) = \frac{1}{2}(\alpha_n \cdot \mathbf{L})$. Using $2(\Lambda^i \cdot \alpha_j)/(\alpha_j \cdot \alpha_j) = \delta_{ij}$ we find the fundamental highest weights to be

$$\Lambda^i = (1, \ldots, \overset{i}{1}, \overset{i+1}{0}, \ldots, 0)$$

for $i = 1, \ldots, n$.

The analysis of $D(\Lambda^i)$, $i = 1, \ldots, n$, is very similar to that of $D(\Lambda^i)$, $i = 1, \ldots, n-1$ of $B(n)$, the weights again having either ± 1 or 0 for their components. However, α_n may be subtracted only once from a weight with 1 as its nth component, to give a weight with -1 for its nth component, so a weight cannot have its number of zero components increased by one. Whenever a weight has a 1 immediately preceding a -1, it is still possible to subtract an α_i, $i \neq n$, twice, one subtraction resulting in a weight with two more zero components. The shell structure of $W(\Lambda^i)$ is therefore similar to the case of $B(n)$, except that only the G_{2k}, $k = 0, \ldots, [i/2]$, occur, i.e.,

$$W(\Lambda^i) = \bigcup_{k=0}^{[i/2]} G_{2k}. \tag{36}$$

Using the dominant weight

$$\mathbf{M}_{2k} = (\overset{1}{1}, \ldots, \overset{i-2k}{1}, 0, \ldots, 0)$$

to calculate the multiplicity of weights of G_{2k}, and the expression $\boldsymbol{\delta} = (n, n-1, \ldots, 2, 1)$, we find that this multiplicity is $((n-i+1)/(n-i+k+1))N_{2k}$, where N_{2k} is as given in Eq. (32). This implies that G_{2k} has total dimension

$$\frac{(n-i+1)}{(n-i+k+1)}\binom{n-i+2k}{k}\binom{n}{i-2k}2^{i-2k}.$$

The total dimension of $D(\Lambda^i)$ is therefore

$$N(\Lambda^i) = \sum_{k=0}^{[i/2]} \frac{(n-i+1)}{(n-i+k+1)}\binom{n-i+2k}{k}\binom{n}{i-2k}2^{i-2k} = \binom{2n}{i} - \binom{2n}{i-2}. \tag{37}$$

Letting

$$\Lambda_j^i = (-1, \ldots, \overset{j}{-1}, 1, \ldots, \overset{i}{1}, 0, \ldots, 0),$$

we find that for $C(n)$, $\Lambda_j^i = \Lambda_{j-1}^i - 2(\alpha_j + \cdots + \alpha_{n-1}) - \alpha_n$, so Λ_j^i is $\{2(n-j)+1\}$ layers down from Λ_{j-1}^i; using this we find that the height of $W(\Lambda^i)$ is given by

$$T(\Lambda^i) = i(2n - i). \tag{38}$$

With the same notation as in the preceding section, and by highly similar methods, it can easily be proved that an arbitrary weight of the type $\mathbf{M}^{h(m_1, \ldots, m_h)}_{2k(l_1, \ldots, l_{i-2k})}$, where $k = 0, \ldots, [i/2]$ and $h = 0, \ldots, i - 2k$, is on the layer ω_j, where now

$$j = \sum_{\lambda=1}^{i-2k} \delta_\lambda^h l_\lambda + (2n+1)(h+k) - \tfrac{1}{2}i(i+1)$$

and hence

$$S_j(\Lambda^i) = \sum_{k=0}^{[i/2]} \frac{(n-i+1)}{(n-i+k+1)} N_{2k} \sum_{h=0}^{i-2k} \times Q(j - (2n+1)(h+k) + \tfrac{1}{2}i(i+1); i-2k, n, h).$$

Property 9 of Section 2 implies the following:

Theorem 4 *For* $i = 1, \ldots, n$,

(a)
$$\sum_{k=0}^{[i/2]} \frac{(n-i+1)}{(n-i+k+1)} N_{2k} \sum_{h=0}^{i-2k} \times Q(j - (2n+1)(h+k) + \tfrac{1}{2}i(i+1); i-2k, n, h)$$
$$= \sum_{k=0}^{[i/2]} \frac{(n-i+1)}{(n-i+k+1)} N_{2k} \sum_{h=0}^{i-2k} \times Q(i(2n-i) - j - (2n+1)(h+k) + \tfrac{1}{2}i(i+1); i-2k, n, h).$$

(b)
$$\sum_{k=0}^{[i/2]} \frac{(n-i+1)}{(n-i+k+1)} N_{2k} \sum_{h=0}^{i-2k} \times \begin{Bmatrix} Q(j - (2n+1)(h+k) + \tfrac{1}{2}i(i+1); i-2k, n, h) \\ -Q(j-1-(2n+1)(h+k) + \tfrac{1}{2}i(i+1); i-2k, n, h) \end{Bmatrix}$$
$$\geq 0, \quad \text{for} \quad 0 \leq j \leq [\tfrac{1}{2}i(2n-i)].$$

As in the case of $B(n)$, (a) holds with the k summation omitted, as can easily be proved using $Q(j; a, b, c) = Q(-j; a, b, a-c)$, so that the shells themselves are layer symmetric, whereas (b) appears to be new.

5. $D(n)$

$D(n)$ is the Lie algebra of the group $O(2n)$, and has rank n. Its positive roots are n-tuples of the form

$$(0, \ldots, 0, \overset{j}{1}, 0, \ldots, 0, \overset{k}{\pm 1}, 0, \ldots, 0)$$

and the simple roots are

$$\alpha_i = (0, \ldots, 0, \overset{i}{1}, \overset{i+1}{-1}, 0, \ldots, 0), \qquad i \neq n$$

and

$$\alpha_n = (0, \ldots, 0, 1, 1).$$

The fundamental weights are easily found to be

$$\Lambda^i = (\overset{1}{1}, \ldots, \overset{i}{1}, \overset{i+1}{0}, \ldots, \overset{n}{0}) \qquad \text{for} \quad i = 1, \ldots, n-2,$$

$$\Lambda^{n-1} = (\tfrac{1}{2}, \ldots, \tfrac{1}{2}, -\tfrac{1}{2}) \qquad \text{and} \qquad \Lambda^n = (\tfrac{1}{2}, \ldots, \tfrac{1}{2}).$$

$W(\Lambda^{n-1})$ and $W(\Lambda^n)$ are rather similar in structure to $W(\Lambda^n)$ of $B(n)$, both having dimension 2^{n-1} and height $(n(n-1)/2)$. $\mathbf{s}_j(\Lambda^{n-1})$ and $\mathbf{s}_j(\Lambda^n)$ are both equal to $P(j; n-1, n-1)$, so application of Property 9 yields Theorem 2, with n replaced by $n-1$. Nothing new is therefore obtained from their analysis.

For $i \leq n-2$, $W(\Lambda^i)$ has a similar structure to $W(\Lambda^i)$ of $C(n)$, with shells G_{2k}, $k = 0, \ldots, [i/2]$, consisting of all n-tuples with $n - i + 2k$ zero components. Freudenthal's formula, with $\delta = (n-1, n-2, \ldots, 1, 0)$, implies that weights of G_{2k} have multiplicity N_{2k}, given in Eq. (32), so here G_{2k} has total dimension

$$\binom{n-i+2k}{k}\binom{n}{i-2k}2^{i-2k}.$$

Summing over all shells, we obtain the following expression for the total dimension of $D(\Lambda^i)$:

$$N(\Lambda^i) = \sum_{k=0}^{[i/2]}\binom{n-i+2k}{k}\binom{n}{i-2k}2^{i-2k} = \binom{2n}{i}, \qquad i = 1, \ldots, n-2. \tag{39}$$

An analogous calculation to those used for $B(n)$ and $C(n)$ leads to

$$T(\Lambda^i) = i(2n - i - 1) \tag{40}$$

and an arbitrary weight of G_{2k} of type $\mathbf{M}^{h(m_1, \ldots, m_h)}_{2k(l_1, \ldots, l_{i-2k})}$, $k = 0, \ldots, [i/2]$, $h = 0, \ldots, i - 2k$, is found to be on the layer ω_j where here

$$j = \sum_{\lambda=1}^{i-2k} \delta^h_\lambda l_\lambda + 2n(k + h) - \tfrac{1}{2}i(i + 1)$$

so

$$s_j(\Lambda^i) = \sum_{k=0}^{[i/2]} N_{2k} \sum_{h=0}^{i-2k} Q(j - 2n(h + k) + \tfrac{1}{2}i(i + 1); i - 2k, n, h) \tag{41}$$

Property 9 implies the following:

Theorem 5 *For* $i = 1, \ldots, n - 2$,

(a) $$\sum_{k=0}^{[i/2]} N_{2k} \sum_{h=0}^{i-2k} Q(j - 2n(h + k) + \tfrac{1}{2}i(i + 1); i - 2k, n, h)$$
$$= \sum_{k=0}^{[i/2]} N_{2k} \sum_{h=0}^{i-2k} Q(i(2n - i - 1) - j - 2n(h + k) + \tfrac{1}{2}i(i + 1); i - 2k, n, h)$$

(b) $$\sum_{k=0}^{[i/2]} N_{2k} \sum_{h=0}^{i-2k} \{Q(j - 2n(h + k) + \tfrac{1}{2}i(i + 1); i - 2k, n, h) - Q(j - 1 - 2n(h + k) + \tfrac{1}{2}i(i + 1); i - 2k, n, h)\}$$
$$\geq 0, \quad \textit{for} \quad 0 \leq j \leq \tfrac{1}{2}i(2n - i - 1).$$

Again, using $Q(j; a, b, c) = Q(-j; a, b, a - c)$, (a) could be proved very easily even with the $\sum_{k=0}^{[i/2]} N_{2k}$ omitted, showing the shells themselves to be layer symmetric, whereas (b) appears to be new. It should be stressed that in (b) of Theorems 3–5, neither the k nor the h summations may be omitted without invalidating the formulas, as simple counterexamples will soon verify.

To summarize, using one theorem concerning representations of the simple Lie algebras, five theorems concerning partitions have been obtained, the part (a) of the theorems being trivially derivable using usual methods, but part (b) being nontrivial. On the other hand, using elementary properties of partitions we have seen that the symmetric part of Dynkin's theorem actually holds not just for the representations but also, in the case of the fundamental representations of $A(n)$, $B(n)$, $C(n)$, and $D(n)$, for the shells of the representations.

The question as to whether new properties of partitions might ensue by applying Dynkin's theorems to arbitrary irreducible, or even reducible, representations of the simple Lie algebras, including in this case also the exceptional Lie algebras, might be worthy of further investigation.

I should like to thank Professor G. E. Andrews of the Pennsylvania State University for encouraging me to write this paper, and for several extremely helpful communications.

REFERENCES

[1] J. W. B. Hughes, A theorem concerning partitions and its consequence in the theory of Lie algebras, *Canad. J. Math.* **20** (1968), 698–700.
[2] S. Chowla, "The Riemann Hypothesis and Hilbert's Tenth Problem." Blackie, London, 1965.
[3] G. Szekeres, An asymptotic formula in the theory of partitions, *Quart. J. Math.* **2** (1951), 85–108.
[4] G. Szekeres, Some asymptotic formulae in the theory of partitions, *Quart. J. Math.* **4** (1953), 96–111.
[5] E. B. Elliott, "Algebra of Quantics," 2nd Ed. Chelsea, New York, 1964.
[6] E. B. Dynkin, Maximal subgroups of the classical groups: Supplement, *Amer. Math. Soc. Transl. Ser. 2* **6** (1957), 245–378.
[7] G. H. Hardy and E. M. Wright, "An Introduction to the Theory of Numbers." Oxford Univ. Press, London and New York, 1938.
[8] H. Rademacher, "Lectures on Elementary Number Theory." Blaisdell, New York, 1964.
[9] N. Jacobson, "Lie Algebras." Wiley (Interscience), New York, 1962.

On Prime Numbers $\equiv$ 1 resp. 3 mod 4

S. KNAPOWSKI†
UNIVERSITY OF MIAMI
MIAMI, FLORIDA

P. TURÁN†
HUNGARIAN ACADEMY OF SCIENCE
BUDAPEST, HUNGARY

1.

For $s = \sigma + it$, $L(s)$ stands throughout this paper for $L(s, \chi_1, 4)$, given for $\sigma > 1$ by

$$\sum_{n=1}^{\infty} \frac{\chi_1(n, 4)}{n^s} = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^s}. \tag{1.1}$$

In our paper [1] we showed that if the Riemann–Piltz conjecture holds for $L(s)$, i.e.,

$$L(s) \neq 0 \qquad \text{for} \quad \sigma > \tfrac{1}{2}, \tag{1.2}$$

then for suitable explicitly calculable positive constants A_1, A_2, and A_3 the inequality

$$\sum_{p>2} (-1)^{(p-1)/2} \log p \exp\left(-A_1 \log^2 \frac{p}{x}\right) < -A_2\sqrt{x} \tag{1.3}$$

holds for all $x > A_3$. This fact gives great interest to the problem to find

† Deceased.

explicitly long sequences of *consecutive* primes $p_\nu, p_{\nu+1}, p_{\nu+2}, \dots, p_{\nu+k}$ with

$$p_\nu \equiv p_{\nu+1} \equiv \cdots \equiv p_{\nu+b} \equiv 1 \bmod 4. \tag{1.4}$$

The longest such sequence below 10^6 was found by Den Haan in Eindhoven consisting of 11 terms; it would be very desirable to find longer such sequences, below 10^8, say.

2.

This problem suggests a number of exciting questions if we add the qualification "infinitely often." The simplest such problem is obviously that concerning

$$f_2(x) \overset{\text{def}}{=} \sum_{\substack{p_\nu \le x \\ p_{\nu-1} \equiv p_\nu \equiv 1 \,(4)}} 1 \tag{2.1}$$

if $x \to \infty$. When asked about the possibility of finding an *elementary* proof of the relation

$$\lim_{x\to\infty} f_2(x) = +\infty \tag{2.2}$$

some years ago, Erdös was definitely very pessimistic about it. As remarked by Ingham on the last page of his book [2], Littlewood's method for proving

$$\overline{\lim_{x\to\infty}} \left(\pi(x) - \int_2^x \frac{dr}{\log r}\right) = +\infty$$

gives—with the usual notations—*mutatis mutandis*

$$\overline{\lim_{x\to\infty}} \{\pi(x, 4, 1) - \pi(x, 4, 3)\} = +\infty$$

$$\underline{\lim_{x\to\infty}} \{\pi(x, 4, 1) - \pi(x, 4, 3)\} = -\infty,$$

which clearly implies (2.2) (and nothing more). Let c stand throughout this paper for positive explicitly calculable numerical constants, not necessarily the same in different occurrences. Then we are going to prove the following

Theorem *For $T > c$, the inequality*

$$f_2(T) > \log^B T$$

holds with positive explicitly calculable constant B.

For $f_3(x)$ defined by

$$f_3(x) = \sum_{\substack{p_\nu \le x \\ p_{\nu-2} \equiv p_{\nu-1} \equiv p_\nu \equiv 1 \,(4)}} 1 \tag{2.3}$$

no proofs are known even for

$$\lim_{x\to\infty} f_3(x) = \infty.$$

It seems to be hopelessly difficult at present to prove for arbitrarily large prescribed ω the existence of *one* sequence $p_\nu, p_{\nu+1}, \cdots, p_{\nu+\omega}$ with

$$p_\nu \equiv p_{\nu+1} \equiv \cdots \equiv p_{\nu+\omega} \equiv 1\ (4). \tag{2.4}$$

This first lower bound for $f_2(T)$ in our theorem is seemingly not very strong, though the (small) exponent B could be considerably improved by a more careful treatment. Much more interesting seems to be our guess that the events

$$p_\nu \equiv p_{\nu+1} \equiv 1\ (4), \qquad p_\nu \equiv p_{\nu+1} \equiv 3\ (4)$$

$$p_\nu \equiv 1\ (4), \quad p_{\nu+1} \equiv 3\ (4), \qquad p_\nu \equiv 3\ (4), \quad p_{\nu+1} \equiv 1\ (4)$$

are "not equally probable." It would be of definite interest—and perhaps feasible in the not too distant future—to prove

$$f_2(x) = o\left(\frac{x}{\log x}\right). \tag{2.5}$$

We shall mention a further problem of localization later.

3.

Now we turn to the proof of our theorem. In our paper [3] we proved the following (see Knapowski and Turán [3, p. 201]). Suppose that in the strip $|t| \le \frac{1}{2}\log^{1/10} T$ the function $L(s)$ has at least one zero in the parallelogram†

$$\sigma \ge \tfrac{1}{2} + \log^{-1/20} T, \qquad |t| \le \tfrac{1}{2}\log^{1/10} T. \tag{3.1}$$

Then we have for $T > c$, numbers U_1, U_2 with

$$(2 <)\ T\exp(-2\log^{15/16} T) \le U_1 < U_2 \le T, \tag{3.2}$$

so that the inequality

$$\sum_{U_1 \le p \le U_2} (-1)^{(p-1)/2} \log p > \sqrt{U_2} \tag{3.3}$$

holds. Let us call a $p_\nu \equiv 1\ (4)$ a "bad" one if $p_{\nu+1} \equiv 3\ (4)$ and a "good" one if $p_{\nu+1} \equiv 1\ (4)$. Associating each bad p_ν with its $p_{\nu+1}$ the contribution of

† In (9.1) of Knapowski and Turán [3] the inequality $|t| \le T$ reads correctly $|t| \le \frac{1}{2}\log^{1/10} T$.

$(\log p_\nu - \log p_{\nu+1})$ being negative can be dropped from the left-hand side of (3.3). The same holds for the contribution of the $p_\nu \equiv 3$ (4) which were not associated with a $p_{\nu-1} \equiv 1$ (4). Hence from (3.3) it follows in the case of (3.1)

$$\{f(U_2) - f(U_1)\} \log U_2 > \sqrt{U_2}$$

and a fortiori

$$f_2(T) > \frac{\sqrt{U_2}}{\log U_2} > \sqrt{T} \exp(-3 \log^{15/16} T) \tag{3.4}$$

for $T > c$. This is much stronger than the inequality of the theorem.

4.

In this first case (3.1) we got also the "local" theorem that the interval

$$[T \exp(-2 \log^{15/16} T),\ T] \tag{4.1}$$

contains a pair $(p_\nu, p_{\nu+1})$ with $p_\nu \equiv p_{\nu+1}$ (4). This was noticed already in Knapowski and Turán [3]. We have now to investigate case II which—owing to the functional equation—means that the roots of $L(s)$ in the strip $|t| \leq \frac{1}{2} \log^{1/10} T$ are contained in the narrow parallelogram

$$|\sigma - \tfrac{1}{2}| < \log^{-1/20} T, \qquad |t| \leq \tfrac{1}{2} \log^{1/10} T. \tag{4.2}$$

For this case we stated in Knapowski and Turán [3] that for $T > c$ and suitable

$$\log_3 T \leq U_2 \exp(-\log^{15/16} U_2) < U_1 < U_2 \leq T \tag{4.3}$$

the inequality

$$\sum_{U_1 \leq p \leq U_2} (-1)^{(p-1)/2} \log p > \sqrt{U_2} \tag{4.4}$$

holds. The proof of (4.3)–(4.4) in case II was on p. 201 of Knapowski and Turán [3], postponed to the English edition of the book of the second author since it was rather long and uses appropriately ideas of Littlewood, Ingham, and Skewes. This will be indeed so (even with $\log_2 T$ instead of $\log_3 T$ in (4.3)), but for our present theorem a much shorter argument can be given (based again on ideas of Littlewood, Ingham, and Skewes essentially).

5.

Let

$$\sum_{n \leq x,\ n \text{ odd}} (-1)^{(n-1)/2} \Lambda(n) \overset{\text{def}}{=} \Delta(x) \tag{5.1}$$

$$\sum_{2 < p \leq x} (-1)^{(p-1)/2} \log p \overset{\text{def}}{=} \Delta_1(x). \tag{5.2}$$

Obviously,

$$\Delta_1(x) = \Delta(x) - \sum_{p \le \sqrt{x}} \log p + O(x^{1/3} \log x) = \Delta(x) - (1 + o(1))\sqrt{x}.$$

Hence if for a $\xi > c$ we have

$$\Delta(\xi) > 3\sqrt{\xi} \tag{5.3}$$

then also $\Delta_1(\xi) > \sqrt{\xi}$ holds and the reasoning of Section 3 gives

$$f_2(\xi) > \sqrt{\xi}/(\log \xi). \tag{5.4}$$

Hence we have to produce in case II, i.e., under supposition (4.2) a possibly large $\xi \le T$ satisfying (5.3).

6.

In order to do this we write

$$\Delta(e^{\vartheta})e^{-\vartheta/2} \overset{\text{def}}{=} G(\vartheta) \tag{6.1}$$

and we start with the "exact" formula of Riemann–Mangoldt in the finitised form as one can find, e.g., in Prachar's book "Primzahlverteilung," p. 228. Restricting us to

$$\log\log\log T \le \vartheta \le \tfrac{1}{10} \log\log T \tag{6.2}$$

(to which we are forced by (4.2)) and denoting the nontrivial zeros of $L(s)$ by

$$\rho = \beta + i\gamma \tag{6.3}$$

we get from it easily

$$G(\vartheta) = -\sum_{|\gamma| \le (1/2)\log^{1/10} T} \frac{e^{(\rho-(1/2))\vartheta}}{\rho} + o(1). \tag{6.4}$$

Now we can use (4.2). We get

$$\left|\frac{e^{(\rho-(1/2))\vartheta}}{\rho} - \frac{e^{i\gamma\vartheta}}{i\gamma}\right| \le \left|\frac{e^{(\rho-(1/2))\vartheta} - e^{i\gamma\vartheta}}{\rho}\right| + \left|\frac{1}{\rho} - \frac{1}{i\gamma}\right|$$

$$\le \frac{1}{|\gamma|}\left\{\exp\left(\frac{\vartheta}{\log^{1/20} T}\right) - 1\right\} + \frac{1}{|\gamma|^2};$$

owing to (6.2) and (6.4), this gives under (4.2)–(6.2)

$$\left|G(\vartheta) + \sum_{|\gamma| \le (1/2)\log^2 T} \frac{e^{i\gamma\vartheta}}{i\gamma}\right| < c. \tag{6.5}$$

If A is a big constant to be determined later, we form after Ingham the integral

$$H(\omega, A) = \frac{1}{2\pi} \int_{-A/4}^{A/4} G\left(\omega + \frac{y}{A}\right) \left(\frac{\sin(y/2)}{y/2}\right)^2 dy \tag{6.6}$$

where ω is restricted by

$$\log\log\log T \leq \omega - \tfrac{1}{4} < \omega + \tfrac{1}{4} \leq \tfrac{1}{10} \log\log T. \tag{6.7}$$

Using (6.6)–(6.5) and completing the integrals to $(-\infty, +\infty)$ we get, using also the formula

$$\frac{1}{2\pi} \int_{-\infty}^{\infty} \left(\frac{\sin(y/2)}{y/2}\right)^2 e^{i\lambda y}\, dy = \begin{cases} 1 - |\lambda| & \text{for } -1 \leq \lambda \leq +1 \\ 0 & \text{for } |\lambda| > 1 \end{cases}$$

of Fejér, the inequality

$$\left| H(\omega, A) + \sum_{|\gamma| \leq A} \frac{e^{i\gamma\omega}}{i\gamma} \right| < c\left(1 + \sum_{|\gamma| \leq (1/2)\log^{1/10} T} \frac{1}{|\gamma|}\right) \left| \int_{A/4}^{\infty} \left(\frac{\sin(y/2)}{y/2}\right)^2 \exp(i(\gamma/A)y)\, dy \right|. \tag{6.8}$$

Since the contribution of the terms with $|\gamma| \leq A$ to the last sum is

$$< \frac{c}{A} \sum_{|\gamma| \leq A} \frac{1}{|\gamma|} < c\frac{\log^2 A}{A} < c$$

and those of the terms with $A < |\gamma| \leq \frac{1}{2} \log^{1/10} T$ after partial integration

$$< \sum_{A \leq |\gamma| \leq (1/2)\log^{1/10} T} \frac{1}{|\gamma|} \left(\frac{A}{|\gamma|} \frac{1}{A^2} + \frac{1}{|\gamma|}\right) < c,$$

we get from (6.8)

$$\left| H(\omega, A) + 2 \sum_{0 < \gamma \leq A} \frac{\sin \gamma\omega}{\gamma} \right| < c_0 \tag{6.9}$$

where c_0 is an explicitly calculable positive numerical constant (i.e., does not depend on A either), whose value matters somewhat.

7.

We shall need the elegant lemma of Ingham which asserts with

$$\alpha_0 = -\frac{\log^2 A}{A} \tag{7.1}$$

the inequality

$$2 \sum_{0<\gamma\le A} \frac{\sin \gamma\alpha_0}{\gamma} < -\tfrac{1}{2} \log \frac{1}{|\alpha_0|} + c_1 \tag{7.2}$$

(c_1 is the same sort of constants as c_0 was in (6.9)).

8.

Now let A be the smallest constant satisfying the inequalities

$$\frac{\log^2 A}{A} \le \tfrac{1}{4}, \qquad \tfrac{1}{2} \log \frac{A}{\log^2 A} \ge \tfrac{1}{3} \log A, \qquad \tfrac{1}{12} \log A \ge 3, \tag{8.1}$$

further with the constants c_0 and c_1

$$c_0 \le \tfrac{1}{24} \log A, \qquad c_1 \le \tfrac{1}{24} \log A,$$
$$\frac{1}{2\pi} \int_{-A/4}^{A/4} \left(\frac{\sin(y/2)}{y/2} \right)^2 dy \ge \tfrac{1}{2} \tag{8.2}$$

and finally

$$N(A) \ge 1 \tag{8.3}$$

where

$$N(x) = \sum_{0<\gamma\le x} 1.$$

If A^* is the value of this A, (6.9)–(8.2) give

$$H(\omega, A^*) > -2 \sum_{0<\gamma\le A^*} \frac{\sin \gamma\omega}{\gamma} - \tfrac{1}{12} \log A^*. \tag{8.4}$$

9.

Next we choose ω (taking care of (6.7)). Putting

$$q = [800\pi \log A^*] \tag{9.1}$$

Dirichlet's theorem gives the existence of an integer m with

$$\frac{1}{20\pi} q^{-N(A^*)} \log\log T \le m \le \frac{1}{20\pi} \log\log T \tag{9.2}$$

so that for all γ's in (8.4), the inequality

$$\left\{ \frac{\gamma}{2\pi} m \right\} \le \frac{1}{q} \tag{9.3}$$

holds.† With this m we choose

$$\omega = m + \alpha_0 \overset{\text{def}}{=} \omega^*. \tag{9.4}$$

(9.2)–(8.1) assures that (6.7) is not violated for $T > c$. Then we have for all of our γ's with $\alpha_0^* = -(\log^2 A^*)/A^*$

$$\begin{aligned} |\sin \gamma\alpha_0^* - \sin \gamma\omega^*| &= \left|\sin \gamma\alpha_0^* - \sin\left(\gamma\alpha_0^* + 2\pi\frac{m\gamma}{2\pi}\right)\right| \\ &= \left|\sin \gamma\alpha_0^* - \sin\left(\gamma\alpha_0^* + \vartheta\frac{2\pi}{q}\right)\right| < \frac{4\pi}{q}, \end{aligned} \tag{9.5}$$

and hence using (9.5)–(8.1)–(7.2)–(8.2)

$$\begin{aligned} -2\sum_{0<\gamma\le A^*}\frac{\sin \gamma\omega^*}{\gamma} &> -2\sum_{0<\gamma\le A^*}\frac{\sin \gamma\alpha_0^*}{\gamma} - \frac{c}{q}\sum_{0<\gamma\le A^*}\frac{1}{|\gamma|} \\ &> -2\sum_{0<\gamma\le A^*}\frac{\sin \gamma\alpha_0^*}{\gamma} - \tfrac{1}{100}\log A^* \\ &> \tfrac{1}{3}\log A^* - c_1 - \tfrac{1}{100}\log A^* > (\tfrac{1}{4} - \tfrac{1}{100})\log A^*. \end{aligned}$$

Then (6.9) gives from (8.2)

$$H(\omega^*, A^*) > (\tfrac{1}{4} - \tfrac{1}{100})\log A^* - \tfrac{1}{24}\log A^* = (\tfrac{5}{24} - \tfrac{1}{100})\log A^*. \tag{9.6}$$

Going back to $G(x)$ this gives, owing to (8.1)–(8.2),

$$\frac{1}{2\pi}\int_{-A^*/4}^{A^*/4} G\left(\omega^* + \frac{y}{A^*}\right)\left(\frac{\sin(y/2)}{y/2}\right)^2 dy > \tfrac{1}{12}\log A^* > 3.$$

Hence there is an

$$\omega^* - \tfrac{1}{4} < \omega^{**} < \omega^* + \tfrac{1}{4} \tag{9.7}$$

so that

$$\Delta(e^{\omega^{**}})\exp(-\tfrac{1}{2}\omega^{**}) = G(\omega^{**}) > 3,$$

i.e.,

$$\Delta(e^{\omega^{**}}) > 3\exp(\tfrac{1}{2}\omega^{**}). \tag{9.8}$$

Putting

$$\exp(\omega^{**}) = \xi$$

we obtain

$$\Delta(\xi) > 3\sqrt{\xi}$$

† $\{x\}$ denotes as usual the distance of x from the next integer.

and from (5.4)

$$f_2(\xi) > 3\sqrt{\xi}. \tag{9.9}$$

Since from (9.7)–(9.4)–(9.2) for $T > c$

$$\xi < \exp(\omega^* + \tfrac{1}{4}) < 2 \log^{1/20\pi} T < T$$

and

$$\xi > \exp(\omega^* - \tfrac{1}{4}) > \log^c T,$$

these and (9.9) give in case II

$$f_2(T) > f_2(\xi) > \frac{\sqrt{\xi}}{\log \xi} > \log^B T$$

with a positive constant B indeed. This and (3.4) complete the proof of our theorem.

REFERENCES

[1] S. Knapowski and P. Turán, Further developments in the comparative prime number theory II, *Acta Arith.* **10** (1964), 293–313.

[2] A. E. Ingham, "The Distribution of Prime Numbers." Cambridge Tracts in Mathematics, London and New York, 1942.

[3] S. Knapowski and P. Turán, Further developments in the comparative prime number theory VII, *Acta Arith.* **21** (1972), 193–201.

AMS (MOS) 1970 subject classifications: 10H10, 10H15.

Signatures on Frobenius Extensions

MANFRED KNEBUSCH

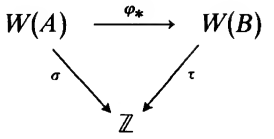
UNIVERSITAET REGENSBURG
REGENSBURG, WEST GERMANY

Introduction

Let A be a commutative ring equipped with an involution J_A. For conciseness, we write A instead of the pair (A, J_A), and denote the ring A without involution by $|A|$. A *signature* σ on A is defined as a homomorphism from the Witt ring $W(A)$ of nondegenerate hermitian forms over A to the ring of integers $\mathbb{Z}$. If $|A|$ has a connected spectrum, either A has no signatures at all or the kernels of the signatures are precisely all minimal prime ideals of $W(A)$, as has been shown in Knebusch [7, I, §2] and Dress [3]. It also can be shown that A has no signatures if and only if -1 is a sum of norms $xJ_A(x)$ in A (proof to be published, cf. [8] for $|A|$ semilocal). In the case that A is a field and J_A is trivial it is well known that the signatures of A correspond uniquely to the orderings of A[5, 11]. For $|A|$ a semilocal ring, a general study of signatures and related topics can be found in Knebusch *et al.* [10] and [8].

For a homomorphism $\varphi: A \to B$ into another ring with involution B an *extension* τ of a signature σ on A to B (with respect to φ) is defined as a

signature τ on B such that the diagram



with φ_* induced by φ is commutative. Recently I developed a theory of "real closures" of a pair (A, σ) with A an arbitrary commutative ring with involution and σ a signature on A (cf. [7]), which generalizes Artin–Schreier's well-known theory of real closures of ordered fields. This theory is tied up with a theory of extensions of σ for φ finite etale {i.e., $|\varphi|\colon |A| \to |B|$ finite etale}. As has been shown in [7] there exist only finitely many extensions of σ to B in this case. Moreover the regular trace $\mathrm{Tr}_{B/A}$ from B to A yields a $W(A)$-linear map

$$\mathrm{Tr}^*_{B/A}\colon W(B) \to W(A),$$

(cf. [12, 7]) and for z in $W(B)$ the following trace formula holds true [7, I, §3]:

$$\sigma(\mathrm{Tr}^*_{B/A}(z)) = \sum_{\tau|\sigma} n(\tau)\tau(z).$$

In this sum τ runs through the extensions of σ to B, and the "multiplicities" $n(\tau)$ are positive integral numbers, uniquely determined by τ and φ. If $|A|$ is semilocal and J_A is trivial, all these multiplicities are 1 [7, II, §8].

Inserting $z = 1$ in this trace formula we see that the number r of signatures of B extending σ is at most equal to the rank $[B : A]$ of the projective A-module B. If $|A|$ is semilocal and $J_A = \mathrm{id}$, moreover $r \equiv [B : A] \bmod 2$.

In the present paper we study the extensions of σ to B in the case that B is a "Frobenius extension" of A. For any element a of a ring with involution we denote the image of a under this involution by $\bar{a}$. We call B a *Frobenius extension* of A if B is as an A-module finitely generated and projective and if there exists a linear form $s\colon B \to A$ on this module such that $s(\bar{b}) = \overline{s(b)}$ for b in B and the hermitian form $s(\bar{x}y)$ on the A-module B is nondegenerate. If the involutions are trivial, this is indeed the usual notion of Frobenius extension occurring in the literature (cf. Eilenberg and Nakayama [4]). We also say that s is a *Frobenius form* on B.

If B is finite etale, the trace $\mathrm{Tr}_{B/A}$ is a Frobenius form on B. But the class of Frobenius extensions is much larger than the class of finite etale extensions. This is the reason the present paper seems to be a necessary step in the theory of hermitian forms over rings. For example, let a be an element in A with $\bar{a} = a$. The extension $B := A[X]/(X^2 - a) = A[x]$ with J_B extending J_A and $\bar{x} = x$ is Frobenius. But if 2 or a is not a unit in A, then B is not etale.

Certainly such extensions are important for a study of hermitian forms. A useful example of a cubic Frobenius extension occurs in [9].

We essentially apply the same methods as in [7], cf. in particular §§3 and 4 of [7], and we use also the terminology and the notations of [7]. Our results are satisfactory only in the case that $|A|$ is semilocal. Much work remains to be done. For example, we do not know in general whether a given signature σ of A has only finitely many extensions to a given Frobenius extension B of A. As has been shown in [7, §3] this is true if B is finite etale over A.

1. The Transfer Formula

In this section A is an arbitrary commutative ring with involution. Let $\varphi: A \to B$ be a Frobenius extension of A and $s: B \to A$ a Frobenius form. Then s induces an additive map

$$s^*: W(B) \to W(A),$$

which is defined as follows. Let (E, Φ) be a hermitian space over B, i.e., a finitely generated projective B-module E equipped with a nondegenerate hermitian form Φ. (Φ is assumed to be antilinear in the first and linear in the second variable.) Then s^* maps the Witt class $[E, \Phi]$ of this hermitian space to the Witt class $[E, s \circ \Phi]$ of the A-module E equipped with the hermitian form $s \circ \Phi$ (cf. Scharlau [12]). Clearly s^* is $W(A)$-linear, i.e., we have

$$s^*(\varphi_*(x)y) = x \cdot s^*(y) \tag{1.1}$$

for x in $W(A)$ and y in $W(B)$.

Now let σ be a signature on A. We denote by $S(\varphi, \sigma)$ the set of all signatures τ of B that extend σ.

Theorem 1.1 *There exists a unique family $(m(\tau) \mid \tau \in S(\varphi, \sigma))$ of integral numbers such that almost all $m(\tau) = 0$ and for every z in $W(B)$ the following equation holds true:*

$$\sigma(s^*(z)) = \sum_{\tau \mid \sigma} m(\tau)\tau(z).$$

Here τ runs through the set $S(\varphi, \sigma)$ of all extensions of σ to B. (If this set is empty, the equation reads $\sigma(s^*(z)) = 0$.)

Proof The kernel $P(\tau)$ of a signature $\tau: W(B) \to \mathbb{Z}$ is a minimal prime ideal of $W(B)$ [3, 7]. Thus there do not exist any inclusion relations between the kernels of different signatures of B. This already implies that there exists at most one family $(m(\tau) \mid \tau \in S(\varphi, \sigma))$ for given φ, σ, s with the above properties; cf. Knebusch [7, I, p. 72].

To prove the existence of such a family $(m(\tau))$ we choose a homomorphism α from A into a real closed field with involution R inducing σ. In more explicit terms this means the following. $|R|$ is an algebraic closed field. J_R is nontrivial, and thus the fixed field R_0 of J_R is a real closed field in the sense of Artin–Schreier. We have

$$W(R) \cong W(R_0) \cong \mathbb{Z}$$

(R_0 equipped with the trivial involution), and denoting the unique signature of R by ρ we have $\rho \circ \alpha_* = \sigma$. Such a homomorphism α exists according to [7, I, §4].

The tensor product $B \otimes_A R$ with respect to φ and α, equipped with the involution $J_B \otimes J_R$, is a Frobenius extension of R with the Frobenius form $s \otimes 1$ from $B \otimes_A R$ to R. It is easily checked that the following diagram commutes:

$$\begin{array}{ccc} W(B) & \xrightarrow{(1\otimes\alpha)_*} & W(B \otimes_A R) \\ {\scriptstyle s*}\downarrow & & \downarrow{\scriptstyle (s\otimes 1)^*} \\ W(A) & \xrightarrow[\alpha_*]{} & W(R) \end{array}$$

We have a unique direct decomposition

$$B \otimes_A R = \prod_{i=1}^{g} B_i$$

into connected rings with involution B_i. Let $\varphi_i\colon R \to B_i$ denote the components of the homomorphism $\varphi \otimes 1$ from R to $B \otimes_A R$, and $\alpha_i\colon B \to B_i$ the components of the homomorphism $1 \otimes \alpha$ from B to $B \otimes_A R$. We may assume that for some r, $0 \leqslant r \leqslant g$ all rings $|B_i|$ with $1 \leqslant i \leqslant r$ are connected and all $|B_i|$ with $r < i \leqslant g$ are not connected. Then for $i > r$, the ring B_i with involution is isomorphic to a product $D_i \times D_i$ of two copies of a ring D_i with the "switch" of the factors as involution. Thus $W(B_i) = 0$ for $i > r$. For $i \leqslant r$, we denote by N_i the nil radical of B_i and we have

$$B_i = \varphi_i(R) \oplus N_i\,.$$

Since 2 is a unit in R and N_i is nilpotent, φ_i induces an isomorphism φ_{i*} from $W(R) \cong \mathbb{Z}$ onto $W(B_i)$ (cf., e.g., [14, Theorem 2.2.1]).

Let $s_i\colon B_i \to R$ denote the restriction of the R-linear form $s \otimes 1$ to the direct summand B_i of the R-module $B \otimes_A R$. Clearly, s_i is a Frobenius form with respect to $\varphi_i\colon R \to B_i$. Denoting finally the projection from $B \otimes_A R$ to B_i, by p_i, the induced maps p_{i*} from $W(B \otimes_A R)$ to $W(B_i)$ yield an

isomorphism

$$(p_{1*}, \ldots, p_{r*})\colon W(B \otimes_A R) \xrightarrow{\sim} \prod_{i=1}^{r} W(B_i),$$

and for u in $W(B \otimes_A R)$ we have

$$(s \otimes 1)^*(u) = \sum_{i=1}^{r} s_i^* p_{i*}(u).$$

Now it is not difficult to prove the desired formula for $\sigma s^*(z)$, with z in $W(B)$. We have

$$\sigma s^*(z) = \rho\alpha_* s^*(z) = \rho(s \otimes 1)^*(1 \otimes \alpha)_*(z)$$

$$= \sum_{i=1}^{r} \rho s_i^* p_{i*}(1 \otimes \alpha)_*(z) = \sum_{i=1}^{r} \rho s_i^* \alpha_{i*}(z).$$

Let γ_i denote the unique homomorphism from B_i to R with $\gamma_i \circ \varphi_i = \mathrm{id}$ $(1 \leqslant i \leqslant r)$. We have $\gamma_{i*} \circ \varphi_{i*} = \mathrm{id}$. Since φ_{i*} is an isomorphism this implies $\varphi_{i*} \circ \gamma_{i*} = \mathrm{id}$. We obtain

$$\sigma s^*(z) = \sum_{i=1}^{r} \rho s_i^* \varphi_{i*} \gamma_{i*} \alpha_{i*}(z) = \sum_{i=1}^{r} \rho s_i^* \varphi_{i*} \beta_{i*}(z),$$

with β_i denoting the homomorphism $\gamma_i \circ \alpha_i$ from B to R. Applying (1.1) this can be simplified to

$$\sigma s^*(z) = \sum_{i=1}^{r} \rho s_i^*(1) \cdot \rho\beta_{i*}(z).$$

Notice that the β_i are precisely all homomorphisms β from the ring with involution B to R with $\beta \circ \varphi = \alpha$. For any signature τ in $S(\sigma, \varphi)$, we denote by $I(\tau)$ the set of all indices i, $1 \leqslant i \leqslant r$, such that $\rho \circ \beta_{i*} = \tau$. Of course only finitely many $I(\tau)$ are nonempty. Further, we denote by $B(\tau)$ the product of all B_i with i in $I(\tau)$. We have

$$B \otimes_A R = \prod_{\tau|\sigma} B(\tau).$$

Finally, we denote by s_τ the restriction of $s \otimes 1$ to the direct summand $B(\tau)$ of the R-module $B \otimes_A R$. Clearly, s_τ is a Frobenius form on the extension $B(\tau)$ of R. Using these notations we can write

$$\sigma s^*(z) = \sum_{\tau|\sigma} m(\tau)\tau(z)$$

with

$$m(\tau) := \rho s_\tau^*(1). \tag{1.2}$$

In more explicit terms, $m(\tau)$ is the signature of the hermitian form $s_\tau(\bar{x}y)$ on the vector space $B(\tau)$ over R.

This proves our Theorem 1.2 and also gives some insight into the nature of the coefficients $m(\tau)$.

The coefficients $m(\tau)$ depend only on φ and τ. We denote them hereafter by $n(\tau, s)$. The notation $n(\tau, \varphi, s)$ or $n(\tau, A, s)$ will be appropriate whenever it is not clear from the context which base ring A is under consideration. The formula

$$\sigma s^*(z) = \sum_{\tau|\sigma} n(\tau, s)\tau(z)$$

will be called the *transfer formula* for $\varphi\colon A \to B$ and s.

From (1.2) we deduce in the case that the rank $[B : A]$ of the projective A-module is constant, the modest information

$$\sum_{\tau|\sigma} |n(\tau, s)| \leqslant [B : A] \tag{1.3}$$

Furthermore,

$$n(\tau, s) \equiv [B(\tau)\colon R] \bmod 2.$$

Thus if $[B : A]$ is constant, we see that

$$\sum_{\tau|\sigma} n(\tau, s) \equiv [B : A] \bmod 2. \tag{1.4}$$

From our proof of the transfer formula also the following corollary is evident.

Corollary 1.2 *Let s be a Frobenius form on B with respect to $\varphi\colon A \to B$. Let σ be a signature on A and τ be an extension of σ to B with $n(\tau, s) \neq 0$. Then for any homomorphism $\alpha\colon A \to R$ into a real closed field with involution R that induces σ there exists a homomorphism $\beta\colon B \to R$ that induces τ and extends α, i.e., $\beta \circ \varphi = \alpha$.*

In general $n(\tau, s)$ may well be zero (cf. Section 2). We mention two cases in which $n(\tau, s) \neq 0$ for all extensions τ of σ to B.

Remark 1.3 If φ is finite etale and s is the regular trace $\mathrm{Tr}_{B|A}$, then all $n(\tau, s)$ are positive numbers. Moreover, given a homomorphism α from A into a real closed field with involution R inducing σ the number $n(\tau, s)$ coincides with the cardinality $n(\tau, \alpha)$ of the set of homomorphisms β from B to R that induce τ and extend α (cf. Knebusch [7, I, §3]). Indeed, in the proof of the transfer formula now the ideals N_i, $1 \leqslant i \leqslant r$, are zero, and the Frobenius forms $s_i\colon B_i \to R$ are the inverse maps of the isomorphisms $\varphi_i\colon R \xrightarrow{\sim} B_i$. This implies immediately $n(\tau, s) = n(\tau, \alpha)$.

If E is an hermitian space† over A of constant rank n then $|\sigma(E)| \leqslant n$ for every signature σ on A. Indeed, let $\alpha: A \to R$ be a homomorphism into a real closed field with involution R inducing σ. Then $\sigma(E)$ is the usual Sylvester signature of the hermitian space $E \otimes_A R$ over R. We call E *positive definite* at σ if $\sigma(E) = n$. Returning to our extension $\varphi: A \to B$ with Frobenius form $s: B \to A$ we denote by $s^*\langle 1\rangle$ the hermitian space B over A, equipped with the hermitian form $s(\bar{x}y)$.

Proposition 1.4 *If B has constant rank over A and $s^*\langle 1\rangle$ is positive definite at σ, then for every signature τ on B extending σ the coefficient $n(\tau, s)$ is positive. Moreover, given a homomorphism α from A to a real closed field with involution R inducing σ we have $n(\tau, s) = n(\tau, \alpha)$.*

Proof Returning to the proof of the transfer formula we see that all spaces $s_i^*\langle 1\rangle$, $1 \leqslant i \leqslant g$, are positive definite over R. Thus $r = g$. Furthermore, the ideals N_i must be zero since otherwise the highest power $N_i^{q_i}$ of N_i that is nonzero would be an isotropic subspace of $s_i^*\langle 1\rangle$. Thus $s_i^*\langle 1\rangle$ has rank one and $s_\tau^*\langle 1\rangle$ has rank $n(\tau, \alpha)$. We obtain

$$n(\tau, s) = \rho s_\tau^*\langle 1\rangle = n(\tau, \alpha).$$

We still have to show $n(\tau, s) > 0$ for a given extension τ of σ to B. We choose a homomorphism β from B into a real closed field with involution R inducing τ, and we put $\alpha := \beta \circ \varphi$. Then certainly $n(\tau, \alpha) > 0$ for this particular τ, hence $n(\tau, s) > 0$. QED

We now look at what happens to the coefficients $n(\tau, s)$ if we replace s by another Frobenius form s' with respect to φ. We have

$$s'(x) = s(bx)$$

where b is an element of B with $\bar{b} = b$ uniquely determined by s and s'. Since the hermitian form $s'(\bar{x}y)$ is nondegenerate, b must be a unit of B. Let $\langle b\rangle$ denote the hermitian space over B consisting of the B-module B and the hermitian form $b\bar{x}y$. We denote the class of this space in $W(B)$ again by $\langle b\rangle$, and the value of this class under a signature τ on B by $\tau(b)$. Clearly

$$s'^*(z) = s^*(\langle b\rangle z)$$

for z in $W(B)$, hence

$$\sigma s'^*(z) = \sum_{\tau|\sigma} n(\tau, s)\tau(\langle b\rangle z) = \sum_{\tau|\sigma} n(\tau, s)\tau(b)\tau(z).$$

Thus we have

$$n(\tau, s') = \tau(b)n(\tau, s) \tag{1.5}$$

for every signature τ on B. Notice that $\tau(b) = \pm 1$ since $\langle b\rangle^2 = 1$.

† We write for brevity E instead of the pair (E, Φ).

2. Some Examples

We first study quadratic extensions. Let A be an arbitrary commutative ring with involution, and let a be a unit in A with $\bar{a} = a$. We consider the ring

$$B := A[T]/(T^2 - a).$$

We have $B = A \oplus At$ with the relation $t^2 = a$. We extend the involution J_A to B either by prescribing $\bar{t} = t$ (case I) or by prescribing $\bar{t} = -t$ (case II).

We introduce the A-linear form s on B with $s(1) = 1$, $s(t) = 0$. Then in both cases $s(\bar{x}) = \overline{s(x)}$ for every x in B. Using the basis $1, t$ of B over A, we obtain

$$s^*\langle 1\rangle \cong \langle 1, a\rangle \qquad \text{(case I)},$$

$$s^*\langle 1\rangle \cong \langle 1, -a\rangle \qquad \text{(case II)}.$$

Thus s is a Frobenius form on B over A.

Let σ be a signature on A.

Proposition 2.1 (i) *Assume $\bar{\ } = t$ If† $\sigma(a) = -1$, then σ has no extension to B. If $\sigma(a) = +1$, then σ has precisely two extensions τ_1, τ_2 to B, and $n(\tau_1, s) = n(\tau_2, s) = 1$.*

(ii) *Assume $\bar{t} = -t$. If $\sigma(a) = +1$, then σ has no extension to B. If $\sigma(a) = -1$, then σ has a unique extension τ to B and $n(\tau, s) = 2$.*

Proof If $\bar{t} = t$, then $a = t\bar{t}$ is a norm in B, and a signature σ on A with $\sigma(a) = -1$ cannot be extended to B. If $\bar{t} = -t$, then $-a = t\bar{t}$ is a norm in B, and a signature σ with $\sigma(a) = +1$ cannot be extended to B. In the remaining cases $s^*\langle 1\rangle$ is positive definite at σ. Thus by Proposition 1.4 every extension τ of σ to B has coefficient $n(\tau, s) > 0$. Furthermore,

$$\sum_{\tau|\sigma} n(\tau, s) = \sigma s^*(1) = 2.$$

Thus one of the following two possibilities must occur:

(A) σ has precisely two extensions τ_1, τ_2, and $n(\tau_1, s) = n(\tau_2, s) = 1$.
(B) σ has a unique extension τ, and $n(\tau, s) = 2$.

Anyway, σ has at least one extension to B, and we choose such an extension τ_1. We further choose a homomorphism β_1 from B to a real closed field with involution R inducing τ_1. We put $\alpha := \beta_1 \circ \varphi$, with φ the inclusion map from A to B. Then α induces σ. Let γ denote the automorphism of B over A of order 2, defined by $\gamma(t) = -t$. Notice that γ is indeed compatible with the involution J_B in both cases. Consider the homomorphism $\beta_2 := \beta_1 \circ \gamma$ from

† Cf. the notations at the end of Section 1.

B to R. We have $\beta_2(t) \neq \beta_1(t)$ and thus β_2 is different from β_1. Clearly, β_1 and β_2 are all homomorphisms from B to R extending α. Let ρ denote the unique signature of R. If $\bar{t} = t$, then we have a hermitian space $\langle t \rangle$ over B consisting of the B-module B and the hermitian form $t\bar{x}y$. We have

$$(\rho \circ \beta_{2*})\langle t \rangle = -(\rho \circ \beta_{1*})\langle t \rangle.$$

Thus there exist two different signature $\rho \circ \beta_{1*}$ and $\rho \circ \beta_{2*}$ extending σ, and possibility (A) is realized. If $\bar{t} = -t$, then

$$\beta_2 = J_R \circ \beta_1.$$

Now J_R is an automorphism of the field with involution R that induces the identity on $W(R)$ (cf. [7, I, Lemma 3.11]). Thus $\rho \circ \beta_{2*} = \rho \circ \beta_{1*} = \tau_1$, and we obtain $n(\tau_1, \alpha) = 2$. According to Proposition 1.4, we have $n(\tau_1, s) = 2$, and possibility (B) is realized.

If $B = A[T]/(T^2 - a)$ but a is not a unit in A, the situation may be very different.

Example 2.2 Let A be the localization of the polynomial ring $\mathbb{R}[x_1, \ldots, x_n]$ in $n \geq 2$ variables x_i with respect to the maximal ideal generated by $x_1, \ldots, x_n$, and let $\mathfrak{m}$ denote the maximal ideal $Ax_1 + \cdots + Ax_n$ of A. We choose the element

$$a := -(x_1^2 + \cdots + x_n^2)$$

in $\mathfrak{m}$ and study the extension

$$B = A \oplus At, \qquad t^2 = a,$$

of A, both A and B being equipped with the trivial involution. The A-linear form s on B defined by $s(1) = 0$, $s(t) = 1$ is a Frobenius form over A. Indeed,

$$s^*\langle 1 \rangle \cong \begin{bmatrix} 0 & 1 \\ 1 & a \end{bmatrix}.$$

The ideal $\mathfrak{M} := \mathfrak{m}B$ is the unique prime ideal of B lying over A, and

$$A/\mathfrak{m} \cong B/\mathfrak{M} \cong \mathbb{R}.$$

We consider the evident signatures attached to $\mathfrak{m}$ and $\mathfrak{M}$.

$$\sigma\colon W(A) \to W(A/\mathfrak{m}) \xrightarrow{\sim} \mathbb{Z}, \qquad \tau\colon W(B) \to W(B/\mathfrak{M}) \xrightarrow{\sim} \mathbb{Z}.$$

Notice that τ extends σ. Since A is regular, σ can also be extended to a signature of the quotient field $\mathbb{R}(x_1, \ldots, x_n)$ of A, equipped with the trivial involution, as has been shown by Craven, Rosenberg, and Ware [2]. Thus there exists an injection α of A into a real closed field with involution R

inducing σ. But this homomorphism α certainly does not extend to a homomorphism β from B to R since $\alpha(a)$ is a negative element of the fixed field R_0 of J_R, and $\beta(t)$ would be an element λ of R_0 with $\lambda^2 = \alpha(a)$. In particular $n(\tau, s) = 0$.

Remark 2.3 From Theorem 3.1 in the next section it can be easily deduced that τ is the only extension of σ to B.

We now shall study extensions of type $B = A[T]/(T^n)$. We have the following general fact.

Lemma 2.4 *Let $\varphi\colon A \to B$ be a homomorphism in the category of commutative rings with involution. Let $\mathfrak{N}_A$ and $\mathfrak{N}_B$ denote the nil radicals of A and B and $\bar{A}$, $\bar{B}$ denote the reductions $A/\mathfrak{N}_A$ and $B/\mathfrak{N}_B$. Assume that φ induces an isomorphism $\bar{\varphi}\colon \bar{A} \to \bar{B}$. Then every signature of A extends in a unique way to a signature of B with respect to φ.*

Proof We have a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ \bar{A} & \xrightarrow[\bar{\varphi}]{} & \bar{B} \end{array}$$

with π and π' the canonical surjections. It suffices to prove the lemma for the homomorphisms π and π'. Then it will be evident for φ too. Thus we assume hereafter that $B = \bar{A}$ and φ is the canonical surjection from A onto $\bar{A}$.

Let σ be a signature on A. We choose a homomorphism α from A into a real closed field with involution R inducing σ. We have a unique homomorphism $\bar{\alpha}$ from $\bar{A}$ to R with $\bar{\alpha} \circ \varphi = \alpha$. Let τ denote the signature on $\bar{A}$ induced by $\bar{\alpha}$. Then τ extends σ. The remaining assertion that τ is the unique extension of σ now follows from the fact that the map φ_* from $W(A)$ to $W(\bar{A})$ is surjective. Since I did not find a reference for this probably well-known fact in full generality, I indicate a proof.

We show that for a given hermitian space (U, h) over $\bar{A}$ there exists a hermitian space (E, Φ) over A whose reduction mod $\mathfrak{N}_A$ is isometric to (U, h). There exists a finitely generated projective A-module E, unique up to isomorphism, such that $E/\mathfrak{N}_A E$ is isomorphic to U (cf., e.g., Swan [13, Theorem 2.26, p. 89]). Thus we assume a priori that U is the reduction $\bar{E}$ of a given finitely generated projective A-module E modulo $\mathfrak{N}_A$. We now can find another hermitian space (V, h') over $\bar{A}$ such that $U \oplus V$ is a free module over $\bar{A}$. Indeed, let W be a module over $\bar{A}$ such that $U \oplus W$ is a free $\bar{A}$-module of finite rank. Then take

$$(V, h') := (U, -h) \perp H(W)$$

with $H(W)$ the hyperbolic space $W \oplus W^*$ constructed from W. (W^* = antidual module of W, $W \oplus W^*$ equipped with the obvious hermitian form which is zero on $W \times W$ and on $W^* \times W^*$.) We again regard V as the reduction mod $\mathfrak{N}_A$ of a finitely generated projective A-module F. The module $G := E \oplus F$ over A is free. Let $g_1, \ldots, g_n$ be a basis of G over A, and let $\bar{g}_1, \ldots, \bar{g}_n$ denote the corresponding basis of the reduction $\bar{G} = U \oplus V$. We now lift the hermitian form $h \perp h'$ of $\bar{G}$ to a hermitian form ψ of G by lifting the hermitian matrix of $h \perp h'$ with respect to the basis $\bar{g}_1, \ldots, \bar{g}_n$ to a hermitian matrix over A in an arbitrary way. Let Φ denote the restriction of ψ to E. Clearly, Φ reduces mod $\mathfrak{N}_A$ to the nondegenerate form h on U, hence Φ itself is nondegenerate. Thus (E, Φ) is a hermitian space over A that has mod $\mathfrak{N}_A$ the reduction (U, h).

Remark If A contains an element μ with $\mu + \bar{\mu} = 1$ (e.g., 2 is a unit in A), then by well-known arguments any two hermitian spaces over A that have isometric reductions mod $\mathfrak{N}_A$ are themselves isometric. Thus the canonical map from $W(A)$ to $W(\bar{A})$ is an isomorphism. We do not need this fact.

We now consider an arbitrary commutative ring A with involution and study the extension $B = A[T]/(T^n)$ for some $n \geqslant 2$. We have

$$B = A \oplus At \oplus \cdots \oplus At^{n-1}, \qquad t^n = 0,$$

and we extend J_A to an involution J_B on B by prescribing $\bar{t} = t$.

Proposition 2.5 *The A-linear form s on B defined by*

$$s(1) = s(t) = \cdots = s(t^{n-2}) = 0, \qquad s(t^{n-1}) = 1$$

is a Frobenius form over A. Every signature σ on A has a unique extension τ to B (cf. the preceding Lemma 2.4). *$n(\tau, s) = 1$ if n is odd, and $n(\tau, s) = 0$ if n is even.*

Proof We have indeed $s(\bar{x}) = \overline{s(x)}$ for x in B. If $n = 2m + 1$, the space $s^*\langle 1\rangle$ has the orthogonal decomposition

$$s^*\langle 1\rangle = (At^m) \perp \mathop{\perp}_{i=0}^{m-1} (At^i + At^{2m-i}).$$

Thus using an obvious notation

$$s^*\langle 1\rangle \cong \langle 1\rangle \perp m \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

If $n = 2m$, we have the orthogonal decomposition

$$s^*\langle 1\rangle = \mathop{\perp}_{i=0}^{m-1} (At^i + At^{2m-1-i})$$

and

$$s^*\langle 1\rangle \cong m \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Thus on the Witt ring level $s^*(1) = 1$ if n odd and $s^*(1) = 0$ if n even. Let now σ be a signature on A and τ be the unique extension of σ to B. By the transfer formula

$$n(\tau, s) = \sigma s_*(1) = \begin{cases} 1, & n \text{ odd} \\ 0, & n \text{ even.} \end{cases}$$

3. Integral Extensions of Semilocal Rings

We now assume that our ring with involution A is semilocal, i.e., $|A|$ has only finitely many maximal ideals. In this case there exists for every signature σ on A a prime ideal $\mathfrak{p}(\sigma)$ of A intimately related to σ, whose definition and relevant properties I want to recall (cf. [7, I, §4 and Appendix B]).

Let A_0 denote the fixed ring of J_A, equipped with the trivial involution. We introduce for σ a given signature on A the set $\Gamma(\sigma)$ consisting of all units a of A_0 with $\sigma(a) = +1$, and the set $Q(\sigma)$ consisting of all finite sums

$$N(\lambda_1)a_1 + \cdots + N(\lambda_r)a_r$$

with a_i in $\Gamma(\sigma)$ and "norms" $N(\lambda_i) = \lambda_i\bar{\lambda}_i$ of elements λ_i of A such that the ideal generated by $\lambda_1, \ldots, \lambda_r$ is the whole of A. Clearly $Q(\sigma)$ is a multiplicative subsemigroup of A_0. Let $-Q(\sigma)$ denote the set of all elements $-x$ with x in $Q(\sigma)$ and $\mathfrak{p}(\sigma)_0$ the complement of $Q(\sigma) \cup (-Q(\sigma))$ in A. The following facts have been proved in [7] and in a more special situation already by Kanzaki and Kitamura [6].

P1 A_0 is the *disjoint* union of $Q(\sigma)$, $-Q(\sigma)$, and $\mathfrak{p}(\sigma)_0$.
P2 $\mathfrak{p}(\sigma)_0$ is a prime ideal of A_0.
P3 The set of all x in A with $N(x)$ lying in $\mathfrak{p}(\sigma)_0$ is a prime ideal $\mathfrak{p}(\sigma)$ of A, obviously stable under J_A, and this is the only prime ideal of A lying over $\mathfrak{p}(\sigma)_0$.
P4 There exists a unique signature $\bar{\sigma}$ on the quotient field $A(\mathfrak{p}(\sigma))$ of the ring with involution $A/\mathfrak{p}(\sigma)$ extending σ with respect to the natural map from A to $A(\mathfrak{p}(\sigma))$.
P5 $\mathfrak{p}(\sigma)$ contains every other prime ideal $\mathfrak{q}$ of A such that $\mathfrak{q}$ is stable under the involution of A and σ extends to some signature on $A(\mathfrak{q})$.

Let σ_0 denote the restriction of σ to A_0. Since the natural map from $W(A_0)$ to $W(A)$ is surjective, σ is the only extension of σ_0 to A. Clearly $\Gamma(\sigma_0)$ coincides with $\Gamma(\sigma)$.

P6 $Q(\sigma_0)$ coincides with $Q(\sigma)$ and $\mathfrak{p}(\sigma_0)$ coincides with $\mathfrak{p}(\sigma)_0$. The natural map from $A_0(\mathfrak{p}(\sigma)_0)$ to $A(\mathfrak{p}(\sigma))$ identifies $A_0(\mathfrak{p}(\sigma)_0)$ with the fixed field $A(\mathfrak{p}(\sigma))_0$ of the involution of $A(\mathfrak{p}(\sigma))$. The signature $\bar{\sigma}$ is the unique extension of $\bar{\sigma}_0$ to $A(\mathfrak{p}(\sigma))$.

P7 $\Gamma(\bar{\sigma}_0)$ is the set of all fractions $\bar{u}\bar{v}^{-1}$ with $\bar{u}$, $\bar{v}$ the images in $A_0/\mathfrak{p}(\sigma)_0$ of elements u, v of $Q(\sigma)$. Notice that $\Gamma(\bar{\sigma}_0)$ is just the set of positive elements of the ordering of $A_0(\mathfrak{p}(\sigma)_0)$ corresponding to $\bar{\sigma}_0$.

P8 Every element s of $Q(\sigma)$ can be written in the form

$$s = a_1 + N(\lambda_2)a_2 + \cdots + N(\lambda_r)a_r$$

with $a_1, \ldots, a_r$ in $\Gamma(\sigma)$ and $\lambda_2, \ldots, \lambda_r$ in A. (If A_0 has no residue class fields with fewer than four elements, then even $s = a_1 + a_2$ with a_1, a_2 in $\Gamma(\sigma)$.)

P9 $\Gamma(\sigma)$ is the intersection of $Q(\sigma)$ and the set A_0^* of units in A_0.

P10 $Q(\sigma) + \mathfrak{p}(\sigma)_0 = Q(\sigma)$.

P11 For x in A but x not in $\mathfrak{p}(\sigma)$, the norm $N(x)$ lies in $Q(\sigma)$.

We call $\mathfrak{p}(\sigma)$ (resp. $\mathfrak{p}(\sigma)_0$) the *prime ideal* of A (resp. of A_0) *associated* with σ.

Let now $\varphi\colon A \to B$ be a homomorphism from A to another semilocal ring with involution B, and let $\varphi_0\colon A_0 \to B_0$ denote the restriction of φ to the fixed rings of the involutions. Let further τ be a signature on B and let σ denote the restriction $\tau \circ \varphi_*$ of τ to A with respect to φ.

Theorem 3.1 *Assume φ is integral, i.e., every element of B is integral over the subring $\varphi(A)$. Then $\mathfrak{p}(\sigma)$ is the preimage of $\mathfrak{p}(\tau)$ under φ, and $\mathfrak{p}(\sigma)_0$, resp. $Q(\sigma)$, are the preimages of $\mathfrak{p}(\tau)_0$, resp. $Q(\tau)$, under φ_0.*

Proof $\mathfrak{p}(\tau)$ is the unique prime ideal of B lying over $\mathfrak{p}(\tau)_0$, and $\mathfrak{p}(\sigma)$ is the unique prime ideal of A lying over $\mathfrak{p}(\sigma)_0$. Thus it suffices to prove the statements about $\mathfrak{p}(\sigma)_0 = \mathfrak{p}(\sigma_0)$ and $Q(\sigma) = Q(\sigma_0)$. Replacing φ by φ_0, we assume without loss of generality that A and B both have trivial involutions.

Without any assumption about φ it is clear that $Q(\sigma)$ is contained in $\varphi^{-1}Q(\tau)$ and $-Q(\sigma)$ is contained in $\varphi^{-1}(-Q(\tau))$. Considering the complement of $Q(\sigma) \cup (-Q(\sigma))$ in A we learn that $\mathfrak{p}(\sigma)$ contains $\varphi^{-1}\mathfrak{p}(\tau)$. (This also follows from the fact that σ extends to a signature on $B(\mathfrak{p}(\tau))$ with respect to the obvious map.) To finish the proof of the theorem it will suffice to show that $Q(\sigma)$ coincides with $\varphi^{-1}Q(\tau)$. Indeed, considering again the complement of $Q(\sigma) \cup (-Q(\sigma))$ in A, this will imply that also $\mathfrak{p}(\sigma)$ coincides with $\varphi^{-1}\mathfrak{p}(\tau)$.

Suppose there exists an element t in $\varphi^{-1}Q(\tau)$ that does not lie in $Q(\sigma)$. Clearly, t also does not lie in $-Q(\sigma)$ since this set is contained in

$\varphi^{-1}(-Q(\tau))$. Thus t must lie in $\mathrm{p}(\sigma)$. On the other hand, we have an equation (cf. P8)

$$\varphi(t) = b_1 + \lambda_2^2 b_2 + \cdots + \lambda_r^2 b_r \qquad (*)$$

with $b_1, \ldots, b_r$ in $\Gamma(\tau)$ and $\lambda_2, \ldots, \lambda_r$ in B.

We consider the field $L := B(\mathrm{p}(\tau))$, equipped with the ordering corresponding to the signature $\bar{\tau}$. For b in B, we denote the natural image in L by $\tilde{b}$; and for a in A, we denote the natural image of $\varphi(a)$ in L also by $\tilde{a}$ for conciseness. We now make the following observation. Let a be an arbitrary element of A. Then $1 - at$ lies in $Q(\sigma)$ since t lies in $\mathrm{p}(\sigma)$ (cf. P10). Thus $1 - \varphi(at)$ lies in $Q(\tau)$, and the element $1 - \tilde{a}\tilde{t}$ in L is positive. Now $\tilde{b}_1 > 0$ and, according to $(*)$, $\tilde{b}_1 \leqslant \tilde{t}$. Thus we learn that

$$\tilde{a}\tilde{b}_1 < 1$$

for every a in A. Introducing the element $d := b_1^{-1}$ of B_1 we have

$$\tilde{a} < \tilde{d} \qquad (**)$$

for every a in A. But this is impossible since B is integral over A. Indeed, we have an equation

$$d^n + \varphi(a_1)d^{n-1} + \cdots + \varphi(a_n) = 0$$

with some $n \geqslant 1$ and elements a_i of A. This implies the equation

$$\tilde{d}^n + \tilde{a}_1\tilde{d}^{n-1} + \cdots + \tilde{a}_n = 0. \qquad (***)$$

Consider the element

$$c := 1 + \varepsilon_1 a_1 + \cdots + \varepsilon_n a_n$$

with $\varepsilon_i = +1$ if $\tilde{a}_i \geqslant 0$ and $\varepsilon_i = -1$ if $\tilde{a}_i < 0$. Then in an obvious notation

$$\tilde{c} = 1 + |\tilde{a}_1| + \cdots + |\tilde{a}_n|.$$

By a well-known lemma the equation $(***)$ implies† $\tilde{d} \leqslant \tilde{c}$, which contradicts $(**)$. Thus an element t as above cannot exist, and we have $Q(\sigma) = \varphi^{-1}Q(\tau)$. This finishes the proof of Theorem 3.1.

This theorem has the following consequence which is important in view of the preceding sections.

Corollary 3.2 *We assume again that $\varphi\colon A \to B$ is an integral homomorphism between semilocal rings, that σ is a signature on A, and τ an extension of σ to B. Let α be a homomorphism from A to a real closed field with involution R that induces σ and has kernel $\mathrm{p}(\sigma)$. (Such a homomorphism clearly exists.) If the field $L := B(\mathrm{p}(\tau))$ has trivial involution or if the field $K := A(\mathrm{p}(\sigma))$ has nontrivial involution, then there exists a unique homomorphism β from B to R*

† In fact, $\tilde{d} \leqslant \mathrm{Max}(1, |\tilde{a}_1| + \cdots + |\tilde{a}_n|)$.

that extends α, i.e., $\alpha = \beta \circ \psi$, and induces τ. In the remaining case that K has trivial involution but L has nontrivial involution there exist precisely two such homomorphisms β_1 and β_2, and $\beta_2 = J_R \circ \beta_1$.

Proof α factors through a unique homomorphism $\bar{\alpha}$ from K to R, and $\bar{\alpha}$ induces the signature $\bar{\sigma}$ on K. The field L is an algebraic extension of K and the signature $\bar{\tau}$ of L extends $\bar{\sigma}$. We want to investigate how many homomorphisms $\bar{\beta}$ from L to R exist that extend $\bar{\alpha}$ and induce $\bar{\tau}$. This is possible by the classical Artin–Schreier theory of orderings and real closures.

Assume first that L, hence also K, has trivial involution. Then $\bar{\alpha}$ maps K into the field R_0 which is real, closed in the classical sense, and also $\bar{\beta}$ must have its image in R_0. By Artin–Schreier's theory there exists a unique homomorphism $\bar{\beta}$ from L to R_0 that extends $\bar{\alpha}$ and induces $\bar{\tau}$.

Assume now that K, hence also L, has nontrivial involution. Let $\bar{\alpha}_0 \colon K_0 \to R_0$ be the restriction of $\bar{\alpha}$ to K_0. Again we have a unique homomorphism $\bar{\beta}_0$ from L_0 to R that extends $\bar{\alpha}_0$ and induces the signature $\bar{\tau}_0$ on L_0 ($\bar{\tau}_0 :=$ restriction of $\bar{\tau}$ = signature induced on $B_0(\mathfrak{p}(\tau_0))$ by τ_0). Now L is the tensor product of L_0 and K over K_0. Thus there exists a unique homomorphism $\bar{\beta}$ from L to R that extends both $\bar{\alpha}$ and $\bar{\beta}_0$. The signature induced on L by $\bar{\beta}$ extends $\bar{\tau}_0$ and thus coincides with $\bar{\tau}$. Clearly $\bar{\beta}$ is the unique homomorphism from L to R that extends $\bar{\alpha}$ and induces $\bar{\tau}$.

Assume finally that K has trivial involution and L has nontrivial involution. We have a unique homomorphism $\bar{\beta}_0$ from L_0 to R that extends $\bar{\alpha}$ and induces $\bar{\tau}_0$. There exist precisely two homomorphisms $\bar{\beta}_1$ and $\bar{\beta}_2$ from L to R that extend $\bar{\beta}_0$ since L is a quadratic extension of L_0 and $|R|$ is algebraically closed, and $\bar{\beta}_2 = J_R \circ \bar{\beta}_1$. Both homomorphisms induce signatures on L that extend $\bar{\tau}_0$. Thus these signatures both coincide with $\bar{\tau}$.

In this way we have found the homomorphisms $\bar{\beta}$ from L to R that induce $\bar{\tau}$ and extend $\bar{\alpha}$ in all cases. Composing these homomorphisms $\bar{\beta}$ with the natural map from B to L we obtain all homomorphisms from B to R that have kernel $\mathfrak{p}(\tau)$, induce τ on B, and extend α.

To complete the proof of our corollary it remains to be shown that any homomorphism β from B to R that extends α and induces τ has kernel $\mathfrak{p}(\tau)$. Let $\mathfrak{q}$ denote the kernel of β. Then $\mathfrak{q}$ lies over the prime ideal $\mathfrak{p}(\sigma)$ of A. Furthermore, we obtain from β a signature on $B(\mathfrak{q})$ that extends τ. Thus $\mathfrak{q} \subset \mathfrak{p}(\tau)$. Since also $\mathfrak{p}(\tau)$ lies over $\mathfrak{p}(\sigma)$ the prime ideals $\mathfrak{p}(\tau)$ and $\mathfrak{q}$ must be equal, according to a well-known theorem of Cohen–Seidenberg about prime ideals of integral extensions (e.g., [1, §2, 1, Corollary 2]).

From this Corollary 3.2, now proved, we obtain immediately

Corollary 3.3 *Let $\varphi \colon A \to B$ be a finite homomorphism between semilocal rings with involution, and assume that B can be generated as a module over A by n elements. Then an arbitrary signature on A has at most n extensions to B.*

Indeed, just observe that in the situation of Corollary 3.2 the homomorphisms from B to R that extend α correspond one to one with the homomorphisms from $B \otimes_A A(\mathfrak{p})$ to R that extend the homomorphism $\bar{\alpha}$ from $A(\mathfrak{p})$ to R induced by α. The algebra $B \otimes_A A(\mathfrak{p})$ has rank at most n over $A(\mathfrak{p})$.

If we study the extensions of a signature σ on A with respect to our integral homomorphism $\varphi: A \to B$, we may pass from A and B to their localizations with respect to $\mathfrak{p}(\sigma)$. This is a consequence of the following localization lemma.

Lemma 3.4 *Let σ be a signature of the semilocal ring with involution A, and let S be a multiplicative subset (= subsemigroup) of $Q(\sigma)$. Assume that the localization $S^{-1}A$ of A with respect to S is again semilocal. Then there exists a unique signature $\tilde{\sigma}$ of $S^{-1}A$ extending σ with respect to the natural map from A to $S^{-1}A$. We have $\mathfrak{p}(\tilde{\sigma}) = S^{-1}\mathfrak{p}(\sigma)$, $\mathfrak{p}(\tilde{\sigma})_0 = S^{-1}\mathfrak{p}(\sigma)_0$, and $Q(\tilde{\sigma}) = S^{-1}Q(\sigma)$.*

Proof Since the natural map from A to $A(\mathfrak{p}(\sigma))$ factors through the map from A to $S^{-1}A$, there exist extensions of σ to $S^{-1}A$. Let τ be one of them. Clearly, $S^{-1}\Gamma(\sigma)$ is contained in $\Gamma(\tau)$, hence $S^{-1}Q(\sigma)$ is contained in $Q(\tau)$. Let u be a unit of the fixed ring $S^{-1}A_0$ of the involution of $S^{-1}A$. The set $S^{-1}A_0$ is the disjoint union of the prime ideal $S^{-1}\mathfrak{p}(\sigma)_0$ and the sets $\pm S^{-1}Q(\sigma)$. Thus u lies in one of the sets $\pm S^{-1}Q(\sigma)$. According to Property P9, applied to τ, we have $\tau(u) = +1$ if u lies in $S^{-1}Q(\sigma)$, and $\tau(u) = -1$ if u lies in $-S^{-1}Q(\sigma)$. Since τ is determined by the values on the hermitian spaces of rank one [Knebusch *et al.* 10, Proposition 2.16], we see that τ is the only signature of $S^{-1}A$ extending σ.

We have a natural map from $S^{-1}A$ to $A(\mathfrak{p}(\sigma))$ that identifies the field $A(\mathfrak{p}(\sigma))$ with the residue class field of $S^{-1}A$ with respect to the prime ideal $S^{-1}\mathfrak{p}(\sigma)$. The restriction of the signature $\bar{\sigma}$ on $A(\mathfrak{p}(\sigma))$ to $S^{-1}A$ is an extension of σ and thus coincides with τ. This implies that $S^{-1}\mathfrak{p}(\sigma)$ is contained in $\mathfrak{p}(\tau)$. We now know that $S^{-1}\mathfrak{p}(\sigma)_0$ is contained in $S^{-1}\mathfrak{p}(\tau)_0$ and from above that $S^{-1}Q(\sigma)$ is contained in $Q(\tau)$. Since $S^{-1}A_0$ is the disjoint union of the sets $S^{-1}\mathfrak{p}(\sigma)_0$, $\pm S^{-1}Q(\sigma)$, and also the disjoint union of the sets $\mathfrak{p}(\tau)_0$, $\pm Q(\tau)$, we have

$$S^{-1}\mathfrak{p}(\sigma)_0 = \mathfrak{p}(\tau)_0, \qquad S^{-1}Q(\sigma) = Q(\tau).$$

It remains to be shown that $S^{-1}\mathfrak{p}(\sigma)$ coincides with $\mathfrak{p}(\tau)$. Let x be an element of $S^{-1}A$ that does not lie in $S^{-1}\mathfrak{p}(\sigma)$. Then $x = s^{-1}y$ with s in S and y in A but y not in $\mathfrak{p}(\sigma)$. According to Property P11, the norm $N(y)$ lies in $Q(\sigma)$, hence $N(x)$ lies in $S^{-1}Q(\sigma)$, which coincides with $Q(\tau)$. Thus, again by P11, x does not lie in $\mathfrak{p}(\tau)$, and we see that the subset $S^{-1}\mathfrak{p}(\sigma)$ of $\mathfrak{p}(\tau)$ actually coincides with $\mathfrak{p}(\tau)$. This finishes the proof of Lemma 3.4.

Proposition 3.5 (i) *Let $\varphi: A \to B$ be a finite homomorphism between semilocal rings with involution. Let σ be a signature on A and let $\mathfrak{p}$ denote the associated prime ideal $\mathfrak{p}(\sigma)$. Then σ has a unique extension $\tilde{\sigma}$ to $A_{\mathfrak{p}}$, and every*

extension τ of σ to B has a unique extension $\tilde{\tau}$ to $B_{\mathfrak{p}}$. Thus we have a one-to-one correspondence between the extensions of σ to B and the extensions of $\tilde{\sigma}$ to $B_{\mathfrak{p}}$.

(ii) *The set $Q(\tilde{\tau})$ consists of the elements uv^{-1} with u in $Q(\tau)$ and v in $Q(\sigma)$, and $\mathfrak{p}(\tilde{\tau})$ is the localization $\mathfrak{p}(\tau)B_{\mathfrak{p}}$ of $\mathfrak{p}(\tau)$.*

(iii) *Assume that in addition φ is a Frobenius extension and that s is a Frobenius form on B over A. Let $\tilde{s}\colon B_{\mathfrak{p}} \to A_{\mathfrak{p}}$ denote the induced Frobenius form on $B_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$. Then $n(\tau, s) = n(\tilde{\tau}, \tilde{s})$ for every extension τ of σ to B.*

Proof Parts (i) and (ii) of the proposition follow from the preceding lemma, applied to both A and B and the multiplicative set $S := Q(\sigma)$. Indeed, by Property P11 we have $S^{-1}A = A_{\mathfrak{p}}$ and $S^{-1}B = B_{\mathfrak{p}}$. Notice that S is contained in $Q(\tau)$ for every extension τ of σ to B.

Assume now that $s\colon B \to A$ is a Frobenius form over A. For y in $W(A)$, we denote the image in $W(A_{\mathfrak{p}})$ by $\tilde{y}$ and for z in $W(B)$ the image in $W(B_{\mathfrak{p}})$ by $\tilde{z}$. We have

$$\sigma s^*(z) = \tilde{\sigma}(s^*(z))^{\sim} = \tilde{\sigma}(\tilde{s}^*(\tilde{z})) = \sum_{\tau|\sigma} n(\tilde{\tau}, \tilde{s})\tilde{\tau}(\tilde{z}) = \sum_{\tau|\sigma} n(\tilde{\tau}, \tilde{s})\tau(z).$$

Thus indeed $n(\tilde{\tau}, \tilde{s}) = n(\tau, s)$ for all signatures τ on B extending σ.

Example 3.6 Assume in the situation of part (iii) of the preceding proposition that $B_{\mathfrak{p}}$ is finite etale over $A_{\mathfrak{p}}$. Then $n(\tau, s) \neq 0$ for every signature τ on B extending σ. More precisely, $|n(\tau, s)| = 2$ if $A(\mathfrak{p}(\sigma))$ has trivial involution and $B(\mathfrak{p}(\tau))$ has nontrivial involution, and $|n(\tau, s)| = 1$ otherwise.

This follows from our Proposition 3.5 using (1.5) and the determination of the multiplicities $n(\tau)$ for finite etale extensions of semilocal rings in [7, II, Proposition 8.5]. (In [7] it is assumed that A and B are connected. This restriction can be removed easily in our situation.)

Our theory of prime ideals associated with signatures on semilocal rings and the consequences drawn from this theory in the present section immediately generalize to "weakly semilocal rings" as considered in [7]. I call a ring A with involution *weakly semilocal* if A contains a semilocal ring A' (stable under the involution) such that A is integral over A'. Then A is the limit of an inductive system of semilocal rings with involution with finite transition morphisms. Weakly semilocal rings with involution are a more natural category for the present section than semilocal rings with involution since an integral extension of a weakly semilocal ring is again weakly semilocal.

4. Frobenius Extensions with One Generator

Let A be a commutative ring with involution.

Proposition 4.1 *Assume B is a Frobenius extension of A generated by one*

element ϑ; $B = A[\vartheta]$. Let σ be a signature on A and α a homomorphism from B to a real closed field with involution R inducing σ. Then for any extension τ of σ to B and any Frobenius form s on B over A, we have

$$|n(\tau, s)| \leqslant n(\tau, \alpha)$$

with $n(\tau, \alpha)$ denoting the number of homomorphisms β from B to R that extend α and induce τ.

This is an improvement of a previous inequality (1.4). To prove the proposition we run through the proof of Theorem 1.1, and we see that it suffices to show that for the Frobenius extensions B_i of R ($1 \leqslant i \leqslant r$) occurring there we have $\rho s_i^* \langle 1 \rangle = 0$ or $= \pm 1$. Now every B_i is generated over R by one element. Thus our proposition is evident if we verify the following lemma.

Lemma 4.2 *Let B be a finite extension of a real closed field with involution R, and assume that B is generated over R by one element. Then B is a Frobenius extension of R. For any Frobenius form s on B we have $s^*(1) = \pm 1$ if $[B : R]$ is odd and $s^*(1) = 0$ if $[B : R]$ is even.*

Proof $B = R \oplus N$ with N the nil radical of B. We assume $N \neq 0$. Let ϑ be a generator of B over R. We have $\vartheta = c + u$ with c in R, u in N, and u is again a generator of B. Let n denote the smallest natural number with $u^n = 0$ ($n \geqslant 2$). Then $1, u, \ldots, u^{n-1}$ is a basis of B over the field R. Clearly

$$\bar{u} = u(\lambda + v)$$

with λ in R, $\lambda \neq 0$, and v in N. Denoting the unit $\lambda + v$ by ε we have $\varepsilon\bar{\varepsilon} = 1$ since $\bar{\bar{u}} = u$. There exists an element μ in R such that $\mu + \lambda\bar{\mu} \neq 0$. Then $\beta := \mu + \varepsilon\bar{\mu}$ is a unit of B, and $\bar{\beta} = \bar{\varepsilon}\beta$. (This is the classical procedure for solving the equation $\varepsilon = \beta\bar{\beta}^{-1}$.) Introducing the element $t := \beta u$, we have $\bar{t} = t$, and $1, t, \ldots, t^{n-1}$ is again a basis of B over R. We introduce the R-linear form s on B with

$$s(1) = \cdots = s(t^{n-2}) = 0, \qquad s(t^{n-1}) = 1.$$

According to Proposition 2.5 this form is a Frobenius form and $s^*(1) = 1$ if n is odd, $s^*(1) = 0$ if n is even. If s' is another Frobenius form on B, then $s'^*(1) = \pm s^*(1)$ (cf. end of Section 1). This finishes the proof of the lemma.

As a relevant example we consider an extension

$$B = A[T]/f(T)$$

with $f(T)$ a normed polynomial in $A_0[T]$ of degree $n \geqslant 2$. Let t denote the image of T in B. Then $1, t, \ldots, t^{n-1}$ is a free basis of the A-module B. We extend the involution J_A to B prescribing $\bar{t} = t$. We consider the A-linear

form s on B defined by

$$s(1) = s(t) = \cdots = s(t^{n-2}) = 0, \qquad s(t^{n-1}) = 1.$$

The hermitian matrix of the hermitian form $s(\bar{x}y)$ with respect to our basis $1, t, \ldots, t^{n-1}$ has the shape

$$\begin{bmatrix} & & & 1 \\ & 0 & 1 & \\ & \iddots & & \\ & 1 & & * \\ 1 & & & \end{bmatrix}$$

and thus is nonsingular, hence s is a Frobenius form.

We now assume in addition that A is semilocal. Let σ be a signature on A, and let $\mathfrak{p}$ respectively $\mathfrak{p}_0$ denote the prime ideal of A, resp. A_0, associated with σ. Let further K denote the residue class field $A(\mathfrak{p})$, and as always let K_0 denote the fixed field of the involution J_K, which coincides with $A_0(\mathfrak{p}_0)$. The image $\bar{f}(T)$ of our polynomial $f(T) \in A_0[T]$ in $K_0[T]$ has a decomposition

$$\bar{f}(T) = \prod_{i=1}^{s} \bar{p}_i(T)^{e_i}$$

with pairwise different normed irreducible polynomials $\bar{p}_i(T)$ over K_0. Let τ be a signature on B extending σ. Then $\mathfrak{p}(\tau)_0$ is a prime ideal of B_0 lying over $\mathfrak{p}_0$ and thus

$$\mathfrak{p}(\tau)_0 = \mathfrak{p}_0 B_0 + p_j(T)B_0$$

with j uniquely determined by τ, $1 \leqslant j \leqslant s$, and $p_j(T)$ a preimage of $\bar{p}_j(T)$ in $A_0[T]$. Since $\mathfrak{p}(\tau)$ is the unique prime ideal of B lying over $\mathfrak{p}(\tau)_0$, the polynomial $\bar{p}_j(T)$ remains irreducible over K, and

$$\mathfrak{p}(\tau) = \mathfrak{p}B + p_j(T)B.$$

We call $\bar{p}_j(T)^{e_j}$ *the factor of* $f(T)$ *corresponding to* τ.

Proposition 4.3 *Let* $\bar{p}_j(T)^{e_j}$ *be the factor of* $\bar{f}(T)$ *corresponding to* τ. *Then* $n(\tau, s) = \pm 1$ *if* e_j *is odd and* $n(\tau, s) = 0$ *if* e_j *is even.*

Proof We choose a homomorphism α from A to a real, closed field with involution R that has kernel $\mathfrak{p}(\sigma)$ and induces σ. There exist either one homomorphism β or two homomorphisms β, β' from B to R which extend α, and in the second case $\beta' = J_R \circ \beta$ (cf. Corollary 3.2). Let λ denote the image of t under β in both cases. Then $\bar{\lambda} = \lambda$, and λ is a zero of the polynomial $\tilde{p}_j[T]$ obtained from $p_j(T)$ by applying α to the coefficients since β factors through $B(\mathfrak{p}(\tau))$. Going through the proof of Theorem 1.1, we see that with the

notations introduced there

$$B(\tau) = R[T]/(T - \lambda)^{e_j}.$$

Our proposition now follows from Lemma 4.2 or already from Proposition 2.5.

It would be more difficult to determine the sign of $n(\tau, s)$ if e_j were odd. We do not enter into this.

REFERENCES

[1] N. Bourbaki, "Algèbre commutative," Chap. V. Hermann, Paris, 1964.
[2] T. C. Craven, A. Rosenberg, and R. Ware, The map of the Witt ring of a domain into the Witt ring of its field of fractions, *Proc. Amer. Math. Soc.* **51** (1975), 25–30.
[3] A. Dress, The weak local global principle in algebraic K-theory, *Comm. Algebra* **3** (1975), 615–661.
[4] S. Eilenberg and T. Nakayama, On the dimension of modules and algebras II (Frobenius algebras and quasi-Frobenius rings), *Nagoya Math. J.* **9** (1959), 1–16.
[5] D. K. Harrison, "Witt rings." Lecture Notes, Dept. of Math., University of Kentucky, Lexington, 1970.
[6] T. Kanzaki and K. Kitamura, On prime ideals of a Witt ring over a local ring, *Osaka J. Math.* **9** (1972), 225–229.
[7] M. Knebusch, Real closures of commutative rings I, *J. Reine Angew. Math.* **274/275** (1975), 61–89; II, *J. Reine Angew. Math.* **286/287** (1976), 278–313.
[8] M. Knebusch, Generalization of a theorem of Artin-Pfister to arbitrary semilocal rings, and related topics, *J. Algebra* **36** (1975), 46–67.
[9] M. Knebusch, Remarks on the paper "Equivalent topological properties of the space of signatures of a semilocal ring" by A. Rosenberg and R. Ware, *Publ. Math. Debrecen*, to appear.
[10] M. Knebusch, A. Rosenberg, and R. Ware, Signatures on semilocal rings, *J. Algebra* **26** (1973), 208–250.
[11] F. Lorenz and J. Leicht, Die Primideale des Wittschen Ringes, *Invent. Math.* **10** (1970), 82–88.
[12] W. Scharlau, Zur Pfisterschen Theorie der quadratischen Formen, *Invent. Math.* **6** (1969), 327–328.
[13] R. G. Swan, "Algebraic *K*-theory," Lecture Notes Math. 76, Springer-Verlag, Berlin–Heidelberg–New York, 1969.
[14] G. E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, *J. Austral. Math. Soc.* **3** (1963), 1–62.

AMS (MOS) 1970 subject classification: 18F25.

Generalizations of Gauss's Lemma

EMMA LEHMER

BERKELEY, CALIFORNIA

The original Gauss lemma is generalized in various ways: First, by replacing the integers $1, 2, \ldots, (p-1)/2$ *by any subset* a_i *of* $(p-1)/2$ *distinct integers less than a prime* p *such that* $a_j \neq p - a_i$ *and having any desired property enjoyed by half the integers* $< p$*; next by replacing the integers less than* p *by any symmetric (modulo* p*) coset of* kth *power residues of* p*; and finally by replacing the prime* p *by a composite modulus* m *and the integers less than* p *by the totatives of* m*.*

Application is made to criteria for the kth *power character of* 2*, to the quartic reciprocity law, and to the character of a permutation.*

Every textbook in elementary number theory contains a simple and elegant result known as Gauss's lemma. It will be found in a little more general form in Hasse [3] and for our purposes can be stated as follows.

Theorem 1 *Let* $p = 2n + 1$ *be a prime. Let* $S = \{1, 2, \ldots, p-1\}$*, and let* S_1 *and* S_λ *be two half-sets of* S *defined as follows:*

$$S_1 = \{a_1', a_2', \ldots, a_n'\} \qquad \text{with} \quad a_i' \neq p - a_j', \quad a_i' \neq a_j'$$

and

$$S_\lambda = \{a_1'', a_2'', \ldots, a_n''\} \qquad \text{where} \quad a_i'' \equiv \lambda a_i' \pmod{p}.$$

If S_λ *contains* μ_λ *elements that are not in* S_1*, then the Legendre symbol*

$$(\lambda/p) = (-1)^{\mu_\lambda}.$$

Corollary 1 *Let $a_i' = i$ for $i = 1, 2, \ldots, n$, then μ_λ is the number of elements in S_λ that exceed n. This is the original Gauss lemma.*

Corollary 2 *Let $a_i' = 2i - 1$ for $i = 1, 2, \ldots, n$, then μ_λ is the number of even elements in S_λ. This special case will be found in Shanks* [7].

We next generalize Gauss's lemma a little further as follows:

Theorem 2 *Let P be any property enjoyed by half the elements a_i but not by $p - a_i$ of $S = \{1, 2, \ldots, p-1\}$ where p is an odd prime, and let μ_1 and μ_λ be respectively the number of elements in S_1 and S_λ of Theorem 1 that do not possess property P, then*

$$(\lambda/p) = (-1)^{\mu_1 + \mu_\lambda}.$$

If property P is enjoyed by all the elements of S_1, then $\mu_1 = 0$ and μ_λ is the number of elements in S_λ that are not in S_1, which is Theorem 1.

Before proving Theorem 2 and hence Theorem 1 as well, we first generalize it to subsets of the first $p - 1$ integers as follows:

Theorem 3 *Let $p = 2kn + 1$ be a prime, let $a_1 < a_2 < \cdots < a_{2n} < p$ and let*

$$S = \{a_1, a_2, \ldots, a_{2n}\} \qquad \text{with} \quad a_{2n+1-i} = p - a_i$$

be any coset of the kth power residues of p and let λ be a kth power residue of p. Let P be a property enjoyed by half the elements a_i of S, but not by $p - a_i$. Let

$$S_1 = \{a_1', a_2', \ldots, a_n'\} \qquad \text{with} \quad a_i' \neq p - a_j', \quad a_i' \neq a_j'$$

and

$$S_\lambda = \{a_1'', a_2'', \ldots, a_n''\} \qquad \text{where} \quad a_i'' \equiv \lambda a_i' \pmod{p}$$

be two half-sets of S, having respectively μ_1 and μ_λ elements not possessing property P, then

$$(-1)^{\mu_1 + \mu_\lambda} = \begin{cases} \left(\dfrac{\lambda}{p}\right) & \text{if } k \text{ is odd,} \\ \left(\dfrac{\lambda}{p}\right)_{2K} & \text{if } k \text{ is even.} \end{cases}$$

Proof Since $a_i' \neq p - a_j'$, it follows that $a_i'' \not\equiv p - a_j''$ (mod p). If either a_i' or a_i'' does not possess property P, then its complement modulo p must possess property P, but there are μ_1 such elements in S_1, and μ_λ in S_λ. Therefore, the product of all the elements in S_λ

$$\prod_{i=1}^{n} a_i'' \equiv \lambda^n \prod_{i=1}^{n} a_i' \equiv \lambda^n (-1)^{\mu_1} \pi \equiv (-1)^{\mu_\lambda} \pi \pmod{p}$$

where π is the product of all the elements in S, having property P. Since p does not divide π, we have

$$(-1)^{\mu_1+\mu_\lambda} \equiv \lambda^n \equiv \lambda^{(p-1)/2k} \equiv \left(\frac{\lambda}{p}\right)_{2k} \pmod{p}.$$

Since λ is a kth power residue, it will be a $2k$th power residue for k odd if it is a quadratic residue. Hence the theorem follows. If $k = 1$ this becomes Theorem 2.

If all the elements of S_1 satisfy property P, then Theorem 3 is a generalization of Theorem 1 with $k = 1$.

We next give some applications of Theorem 3 in case 2 is a kth power residue.

Theorem 4 *Let $p = 2kn + 1$ and suppose that 2 is a kth power residue of p, then the parity of the number of elements exceeding $p/2$ in a half-coset*

$$S_1 = \{a'_1, a'_2, \ldots, a'_n\} \qquad \text{with} \quad a'_j \neq p - a_i$$

of any coset of kth power residue modulo p is the same as the parity of the number of odd elements in the half coset if and only if 2 is a $2k$th power residue of p.

Proof Let P be the property that an element is less than $p/2$ and let P' be the property that an element is even. Let μ_1 and μ_2 and, correspondingly, μ'_1 and μ'_2 be the number of elements that do not possess property P and P' in S_1 and S_2, respectively. Then by Theorem 3 with $\lambda = 2$ we have

$$(2/p)_{2k} = (-1)^{\mu_1+\mu_2} = (-1)^{\mu_1'+\mu_2'}$$

or

$$\mu_1 + \mu_2 \equiv \mu'_1 + \mu'_2 \pmod{2}.$$

But every element which exceeds $p/2$ in S_1 generates an odd element in S_2, therefore $\mu_1 \equiv \mu'_2$ and hence $\mu_2 \equiv \mu'_1 \pmod 2$ so that

$$(-1)^{\mu_1+\mu_1'} = \begin{cases} (2/p) & \text{when } k \text{ is odd} \\ (2/p)_{2k} & \text{when } k \text{ is even,} \end{cases}$$

which is the theorem.

Corollary *If k is odd, and if 2 is a kth power residue, then $\mu_1 \equiv \mu'_1 \pmod 2$ if and only if $p \equiv \pm 1 \pmod 8$.*

This corollary was first proposed as a problem for $k = 1$, for the set

$$S_1 = \{g^k, g^{2k}, \ldots, g^{nk}\}$$

where g is a primitive root of $p = 2nk + 1$.

Example 1 Let $k = 3$, $p = 31$, $g = 3$, $a'_i = 3^{3i}$ $(i = 1, 2, 3, 4, 5)$.

$$S_1 = \{27, 16, 29, 8, 30\}, \qquad \mu_1 = 4, \quad \mu'_1 = 2.$$

As predicted by the corollary the μ's have the same parity.

Theorem 5 *Let $p = 2nk + 1$, let v_k be the number of elements $< p/4$ in the half-set S_1 of any coset of* kth *power residues, where*

$$S_1 = \{a_1', a_2', \ldots, a_n'\} \qquad \text{with} \quad a_i' < p/2.$$

If 2 is a kth *power residue, then*

$$(-1)^{n+v_k} = \begin{cases} (2/p) & \text{if } k \text{ is odd} \\ (2/p)_{2k} & \text{if } k \text{ is even.} \end{cases}$$

Proof Using Theorem 3 with $\lambda = 2$ we note that for every $a_i'' \equiv 2a_i' \pmod{p}$ which exceeds $p/2$ there is an a_i' that exceeds $p/4$, therefore $v_k = n - \mu_2$, and since $\mu_1 = 0$, the theorem follows.

Corollary *If k is odd, the number of* kth *power residues less than $p/4$ is of the same parity as $(p-1)/2k$ if and only if $p \equiv \pm 1 \pmod 8$.*

For $k = 1$, the theorem is trivial. For $k = 3$, $p = 31$, we have $a_i' = 1, 2, 4, 8, 15$, so that $v_3 = 3$, $30/6 = 5$.

For $k = 2$, there are many expressions for the quartic character of 2 beginning with Gauss in terms of $p = a^2 + 4b^2$, Barrucand and Cohn [1] in terms of $c^2 + 8d^2$ and the class number $h = h(\sqrt{-4p})$, and by Hasse [4] in terms of $h' = h(\sqrt{-8p})$. Since 2 must be a quadratic residue, $p \equiv 1 \pmod 8$, letting $n = 2n'$ in Theorem 5, and we have

$$(-1)^{v_2} = \left(\frac{2}{p}\right)_4 = (-1)^{b/2} = (-1)^{d+n'} = (-1)^{n'+h/4} = (-1)^{h'/4}.$$

For example, for $p = 73$, there are $v_2 = 10$ quadratic residues less than $p/4$, $n' = 9$, $b = 4$, $d = 3$, $h = 4$, $h' = 16$, all testifying to the fact that 2 is a quartic residue of 73.

Going one step further, we find that for $k = 4$, the quartic residues of 73, less than $p/4$, are 1, 2, 4, 8, 16, so that $v_4 = 5$, $n = 9$, and hence 2 is an octic residue of 73 by Theorem 5. It is also well known that $(2/p)_8 = (-1)^{n+b/4}$ so that in general $v_4 \equiv b/4 \pmod 2$.

Another application of Theorem 3 is as follows:

Theorem 6 *The multiplication of the elements of any coset S of* kth *power residues of a prime $p = 2nk + 1$ by a* kth *power residue λ produces an even permutation if and only if*

$$1 = \begin{cases} \left(\dfrac{\lambda}{p}\right) & \text{if } k \text{ is odd} \\ \left(\dfrac{\lambda}{p}\right)_{2k} & \text{if } k \text{ is even.} \end{cases}$$

Proof Since $p = 2kn + 1$, the set S is symmetric modulo p. Let S_1 contain the elements $a_i < p/2$ and S_1' contain the elements $p - a_i$ for $i = 1, 2, \ldots, n$. By Theorem 3, multiplication of $a_i \in S_1$ by λ will contain μ_λ elements that exceed $p/2$, where

$$(-1)^{\mu_\lambda} = \begin{cases} \left(\frac{\lambda}{p}\right) & \text{if } k \text{ is odd} \\ \left(\frac{\lambda}{p}\right)_{2k} & \text{if } k \text{ is even.} \end{cases}$$

If these μ_λ elements of S_λ are interchanged with their complements in the set S_λ', obtained by multiplying the set S_1' by $\lambda \pmod p$, the resulting set will consist of n elements $< p/2$, followed by their complements modulo p. If each half is now subjected to the same interchanges, the parity of the permutation will not change so that the permutation is of the same parity as μ_λ, which proves the theorem.

Corollary *The multiplication by λ of the integers $1, 2, \ldots, p - 1$ produces an even or odd permutation according as λ is a quadratic residue or not.*

This is Zolotareff's theorem [8] which follows from Theorem 5 with $k = 1$, or directly from Theorem 1.

Theorem 6 is applicable to all primes $p \equiv 1 \pmod k$ if k is odd, but only to those $p \equiv 1 \pmod{2k}$ if k is even. However, in the remaining cases k even and $p \equiv k + 1 \pmod{2k}$ the permutation can be shown to be always even by another method.

Gauss made good use of his lemma in his third proof of the law of quadratic reciprocity. If we use Theorem 3 with $\lambda = \lambda(p) = q$ and then again with p replaced by q and with $\lambda(q) = p$, we obtain the following theorem:

Theorem 7 *Let $p = 2nk + 1$, $q = 2km + 1$, and let $(p/q)_k = (q/p)_k = 1$, let $\mu_q(p)$ be the number of elements exceeding $p/2$ among the multiples of the first half of the* k*th power residues of p by q, while $\mu_p(q)$ is the corresponding number of multiples of p by the first half of the* k*th power residues of q that exceed $q/2$ modulo q, then*

$$(-1)^{\mu_p(q) + \mu_q(p)} = \begin{cases} (p/q)(q/p) = (-1)^{(p-1)(q-1)/4} & \text{if } k \text{ is odd} \\ (p/q)_{2k}(q/p)_{2k} & \text{if } k \text{ is even.} \end{cases}$$

Corollary *If k is odd, then*

$$\mu_q(p) \equiv \begin{cases} 1 + \mu_p(q) \pmod 2 & \text{if } p \equiv q \equiv -1 \pmod 4 \\ \mu_p(q) \pmod 2 & \text{otherwise.} \end{cases}$$

When $k = 1$, this is the reciprocity theorem. When $k = 2$, $p = 4n + 1$ we are

dealing with multiples of quadratic residues (or nonresidues) of p and q such that $(p/q) = (q/p) = 1$ and obtain

$$\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = (-1)^{\mu_p(q)+\mu_q(p)}.$$

Other criteria for the quartic reciprocity law are known, such as Burde [2] and Lehmer [6] in terms of $p = a^2 + b^2$, $q = c^2 + d^2$ and of $p = C^2 + qD^2$, when such a representation exists. These are

$$\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4 = (-1)^n\left(\frac{ac-bd}{p}\right) = \begin{cases} 1 & \text{if } q = 8n+1, \quad p = C^2+qD^2 \\ (-1)^D & \text{if } q = 8n+5 \end{cases}$$

so in this case

$$\mu_q(p) \equiv \mu_p(q) \pmod 2 \quad \begin{cases} q = 8n+1, & p = C^2+qD^2 \\ q = 8n+5, & p = C^2+4qD^2 \end{cases}$$

or

$$(-1)^n\left(\frac{ac-bd}{p}\right) = 1.$$

Example $k = 2$, $p = 41$, $q = 37$, $a = 5$, $b = 4$, $c = 1$, $d = 6$, $D = 1$, $(p/q)_4(q/p)_4 = -1$ since the quadratic residues modulo $41 < p/2$ are 1, 2, 4, 8, 9, 10, 16, 18, 20 multiplication by 37 (mod 41) gives 37, 33, 25, 21, 9, 5, 1, 18, 10, 2 of which the first four exceed $p/2$, hence $\mu_{37}(41) = 4$, while the quadratic residues of $37 < q/2$ are 1, 3, 4, 7, 9, 10, 11, 12, 16 multiplication by 41 (mod 37) gives 4, 12, 16, 28, 36, 3, 7, 11, 27 (mod 37) with only three numbers exceeding 18, hence $\mu_{41}(37) = 3$ and the result follows.

In conclusion, we give a generalization to a composite modulus m as follows:

Theorem 8 *Let $m > 4$ and let $n = \phi(m)/2$. Let*

$$S = \{m_1, m_2, \ldots, m_{2n}\}, \qquad m_i < m \quad \text{and} \quad (m_i, m) = 1$$

be the set of totatives of m. Let P be a property enjoyed by half the elements m_i of S, but not by $p - m_i$. And let

$$S_1 = \{m_1', m_2', \ldots, m_n'\} \qquad \text{with} \quad m_i + m_j \not\equiv 0 \pmod m$$

and

$$S_\lambda = \{m_1'', m_2'', \ldots, m_n''\} \qquad \text{where} \quad m_i'' \equiv \lambda m_i' \pmod m$$

be two half-sets of totatives of m having respectively μ_1 and μ_λ elements which

do not possess property P, then

$$(-1)^{\mu_1+\mu_\lambda} = \begin{cases} (\lambda/p) & \text{if } m = p^\alpha \text{ or } 2p^\alpha \\ 1 & \text{otherwise.} \end{cases}$$

Proof Let M be the product of all the totatives of m having property P, and let M_1 and M_λ respectively be the products of all the elements in S_1 and S_λ. Since either m_i' or $m - m_i'$ is an element of S_1 and similarly either m_i'' or $m - m_i''$ is an element of S_λ, it follows that $M_1 \equiv (-1)^{\mu_1} M \pmod{m}$ and that

$$M_\lambda \equiv (-1)^{\mu_\lambda} M \equiv \lambda^n (-1)^{\mu_1} M \pmod{m}.$$

Since $(M, m) = 1$, we obtain

$$(-1)^{\mu_1+\mu_\lambda} \equiv \lambda^n \pmod{m}.$$

But it is known that for $m > 4$,

$$\lambda^n = \lambda^{\phi(m)/2} = \begin{cases} (\lambda/p) & \text{if } m = p^\alpha \text{ or } 2p^\alpha \\ 1 & \text{otherwise,} \end{cases}$$

so that the theorem follows.

Theorem 8 reduces to Theorem 3 with $k = 1$ if $m = p$ and gives a generalization of Zolotareff's theorem mentioned in the corollary to Theorem 6 to a composite modulus as follows:

Theorem 9 *The multiplication of the totatives of $m > 4$ by a number λ prime to m produces an even permutation if $m \neq p^\alpha$ or $2p^\alpha$. In case $m = p^\alpha$ or $2p^\alpha$, the permutation is even or odd according as $(\lambda/p) = 1$ or -1.*

Proof Let S_1 contain the totatives $m_i < m/2$ of m and S_1' those that exceed $m/2$ and let property P be that $m_i < m/2$, then $\mu_1 = 0$ in Theorem 8 and μ_λ is the number of elements in S_λ that exceed $m/2$. If these elements are interchanged with the corresponding elements in S_λ' obtained by multiplying S_1' by λ, the resulting half-sets will contain elements $m_i'' < m/2$ followed by $m - m_i'' > m/2$. The permutation can now be completed by making corresponding interchanges in both sets, so that the parity of the permutation is exactly μ_λ and the theorem follows from Theorem 8.

For example, for $m = 18$, $n = 3$, $\lambda = 5$, $S = \{1, 5, 7, 11, 13, 17\}$, $S_1 = \{1, 5, 7\}$, $S_1' = \{11, 13, 17\}$, $S_5 = \{5, 7, 17\}$, $S_5' = \{1, 11, 13\}$, and $\mu_1 = 0$, $\mu_5 = 1$, so that there is an odd number of interchanges. In fact, we interchange 1 and 17, then 1 and 5 and 13 and 17, and finally 5 and 7 and 11 and 13, so there are actually five interchanges and since $m = 2 \cdot 3^2$, $p = 3$ and $(\lambda/p) = (5/3) = -1$.

To avoid confusion, it should be noted that Hasse's [5] generalization of Gauss's lemma to composite modulus finds the parity of the number N of solutions (x, y) of the inequality $\lambda x - my < 0$ with $x < m/2$ and prime to m

and $y < \lambda/2$ for λ a prime. It turns out that $N \equiv \mu_\lambda \pmod 2$ unless $p = 2p^\alpha$ in which case N is always even, while μ_λ is odd in case $(\lambda/p) = -1$ as in the above example. On the other hand, for $\lambda = 5$, $m = 18$ we have the solutions (1, 1), (1, 2), (5, 2), and (7, 2), giving $N = 4$.

REFERENCES

[1] P. Barrucand and H. Cohn, Note on primes of the type $x^2 + 32y^2$, *J. Reine Angew. Math.* **238** (1969), 67–70.
[2] Klaus Burde, Ein retionales biquadratishes Reziprozitatsgesetz, *J. Reine Angew. Math.* **235** (1969), 175–184.
[3] H. Hasse, "Vorlesungen Uber Zahlentheorie," Chap. 2, Section 6.
[4] H. Hasse, Uber dis Klassenzahl des Korpers $P(\sqrt{-2p})$ mit ein Primzahl $p \neq 2$, *J. Number Theory* **1** (1969), 231–234.
[5] H. Hasse, "Uber die Klassenzahl abelisher Zahlkörper," pp. 84–87. Akademishe Verlag, Berlin, 1952.
[6] Emma Lehmer, On some special quartic reciprocity laws, *Acta Arith.* **21** (1972), 367–377.
[7] Daniel Shanks, "Solved and Unsolved Problems in Number Theory," Vol. 1, p. 39.
[8] E. I. Zolotareff, Nouvelle demonstration de la loi de réciprocité de Legendre, *Nouvelles Ann. Math.* **11** (1872), 354–362.

On $|\alpha|^2 + |\beta|^2 = p^t$ in Certain Cyclotomic Fields

SUNDER LAL

PANJAB UNIVERSITY
CHANDIGARH, INDIA

R. L. McFARLAND

WRIGHT STATE UNIVERSITY
DAYTON, OHIO

R. W. K. ODONI

UNIVERSITY OF EXETER
EXETER, ENGLAND

Let p be a prime of the form $4k + 3$ and let s, t be nonnegative integers. It is shown that any solution to $|\alpha|^2 + |\beta|^2 = p^t$ in the algebraic integers of the cyclotomic field $\mathbb{Q}(e^{2\pi i/p^s})$ must have α or β equal to zero.

Let p be a prime of the form $4k + 3$. It is well known from elementary number theory that the diophantine equation

$$a^2 + b^2 = p^{2t}$$

has only the trivial solutions with a or b equal to zero. In this paper we extend this result to the algebraic integers in the cyclotomic field $\mathbb{Q}(e^{2\pi i/p^s})$

obtained by adjoining a primitive p^sth root of unity to the field $\mathbb{Q}$ of rationals. We prove

Theorem *Let p be a prime of the form $4k + 3$ and let s, t be nonnegative integers. If α and β are algebraic integers in $\mathbb{Q}(e^{2\pi i/p^s})$ that satisfy*

$$|\alpha|^2 + |\beta|^2 = p^t, \tag{1}$$

then either α or β is zero. More generally, the same conclusion holds if

$$|\alpha|^2 + |\beta|^2 = |\rho|^2, \tag{2}$$

where ρ is an algebraic integer in $\mathbb{Q}(e^{2\pi i/p^s})$ that divides some power of p.

Proof Let $\mathbb{Z}$ denote the ring of rational integers and let p be a prime of the form $4k + 3$. If $a^2 + b^2 \equiv 0 \pmod{p}$ with $a, b \in \mathbb{Z}$, then $a \equiv b \equiv 0 \pmod{p}$; for $a \not\equiv 0 \pmod{p}$ would imply that $(b/a)^2 \equiv -1 \pmod{p}$, which is impossible. The diophantine equation $a^2 + b^2 = p^t$ has no solution if t is odd by a mod 4 argument; and if t is even, an easy induction on t shows that either a or b is zero. This proves the theorem for $s = 0$.

Now suppose that s is a positive integer. Let $\zeta = e^{2\pi i/p^s}$. Then $\mathbb{Z}[\zeta]$ is the ring of algebraic integers of $\mathbb{Q}(\zeta)$ and $\mathbb{Z}[\zeta + \bar{\zeta}]$ is the ring of algebraic integers of $\mathbb{Q}(\zeta + \bar{\zeta})$, the maximal real subfield of $\mathbb{Q}(\zeta)$. Furthermore, $\{1, \zeta\}$ is an integral basis of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}(\zeta + \bar{\zeta})$. Let $\alpha, \beta \in \mathbb{Z}[\zeta]$ satisfy (2), where $\rho \in \mathbb{Z}[\zeta]$ is a divisor of some positive integral power of p. For the moment, assume that ρ is not a unit and that the t occurring in (1) is not zero. Note that any positive integral power of p can be expressed in the form $\rho\bar{\rho}$ since $p = \prod_j (1 - \zeta^j)$, where j ranges over a reduced residue system modulo p^s. Write

$$\alpha = a_1 + a_2\zeta, \qquad \beta = b_1 + b_2\zeta, \tag{3}$$

where $a_1, a_2, b_1, b_2 \in \mathbb{Z}[\zeta + \bar{\zeta}]$. The principal ideal generated by p factors in $\mathbb{Z}[\zeta]$ as $(p) = (1 - \zeta)^\phi$, where ϕ denotes the value of the Euler ϕ-function at p^s. Thus $\rho = \varepsilon(1 - \zeta)^r$ for some positive integer r and a unit $\varepsilon \in \mathbb{Z}[\zeta]$. Hence

$$|\rho|^2 = \varepsilon\bar{\varepsilon}\omega^r, \tag{4}$$

where

$$\omega = (1 - \zeta)(1 - \bar{\zeta}) = 2 - (\zeta + \bar{\zeta}). \tag{5}$$

Then (2)–(5) yield

$$\begin{aligned}\alpha\bar{\alpha} + \beta\bar{\beta} &= a_1^2 + a_2^2 + a_1a_2(2 - \omega) + b_1^2 + b_2^2 + b_1b_2(2 - \omega)\\ &= (a_1 + a_2)^2 + (b_1 + b_2)^2 - (a_1a_2 + b_1b_2)\omega\\ &= \varepsilon\bar{\varepsilon}\omega^r.\end{aligned}$$

Therefore, in $\mathbb{Z}[\zeta + \bar{\zeta}]$

$$(a_1 + a_2)^2 + (b_1 + b_2)^2 \equiv 0 \pmod{\omega}.$$

The residue class ring $\mathbb{Z}[\zeta + \bar{\zeta}]/(\omega)$ is a finite field whose order is the norm of ω, that is, p. As noted previously, the equation $a^2 + b^2 = 0$ has only the trivial solution $a = b = 0$ in the field of order $p \equiv 3 \pmod 4$. Hence $a_1 + a_2 \equiv 0 \pmod{\omega}$, say $a_1 + a_2 = \eta\omega$ with $\eta \in \mathbb{Z}[\zeta + \bar{\zeta}]$. Thus

$$\alpha = a_1 + a_2\zeta = a_1 + (\eta\omega - a_1)\zeta = a_1(1 - \zeta) + \eta\omega\zeta.$$

Therefore, $1 - \zeta$ divides α. Similarly, $1 - \zeta$ divides β. Write $\alpha = \alpha_1(1 - \zeta)$, $\beta = \beta_1(1 - \zeta)$, where α_1, β_1 belong to $\mathbb{Z}[\zeta]$ and satisfy

$$|\alpha_1|^2 + |\beta_1|^2 = \varepsilon\bar{\varepsilon}\omega^{r-1}.$$

Proceed by induction on r to obtain

$$|\alpha_r|^2 + |\beta_r|^2 = \varepsilon\bar{\varepsilon}. \tag{6}$$

Let $\alpha_0 = \alpha_r/\varepsilon$, $\beta_0 = \beta_r/\varepsilon$ so that

$$|\alpha_0|^2 + |\beta_0|^2 = 1, \tag{7}$$

with $\alpha_0, \beta_0 \in \mathbb{Z}[\zeta]$. Observe that (1) and (2) are already of the form (7) and (6), respectively, if $t = 0$ or ρ is a unit. The Galois group of $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is abelian, so in particular complex conjugation commutes with algebraic conjugation. Therefore (7) implies that all conjugates of α_0 do not exceed one in absolute value. Hence by a theorem of Kronecker, α_0 is zero or a root of unity; and similarly for β_0. Whence by (7), either α_0 or β_0 is zero. Thus α or β must be zero. This completes the proof.

The theorem is of course false for primes of the form $4k + 1$, for such primes can be expressed as the sum of two squares in $\mathbb{Z}$. Suppose $p = 2$. It is not difficult to show that

$$|\alpha|^2 + |\beta|^2 = 2^t \tag{8}$$

has only trivial integral solutions in $\mathbb{Z}(e^{2\pi i/2^s})$ with α or β zero if and only if t is even and $s = 0$ or 1. Indeed, (8) has a solution with $\alpha = \beta$ in $\mathbb{Z}$ or $\mathbb{Z}[i]$ according as t is odd or even.

AMS (MOS) 1970 subject classifications: 12A05, 12A35.

Galois Cohomology and a Theorem of E. Artin

MANOHAR L. MADAN *SAT PAL*

THE OHIO STATE UNIVERSITY
COLUMBUS, OHIO

1. Introduction

In his dissertation, E. Artin proved [1] that there are only finitely many quadratic extensions $E/k(x)$ for which the ideal class group of the integral closure of $k[x]$ has exponent 2 if k is a prime field of odd characteristic and the infinite prime does not split. The inequalities from which Artin drew the conclusion about the finiteness also give upper bounds on the genera of such fields. D. Madden [4] gave a substantial improvement of these upper bounds. He also included the case of characteristic 2 and allowed k to be any finite field. In Section 3 we give a further improvement of Artin's theorem. The null class group has exponent 2 for such fields 2. Using the class number formula for the ambiguous classes and counting the number of integral divisors in a divisor class of sufficiently large degree, an application of the Riemann hypothesis gives a bound on the genus. If there is no ramified prime of degree one, these bounds are better than those obtained by Madden.

In Section 2 we evaluate the Galois cohomology groups for the null class group and the divisor class group associated with a cyclic extension E/F of prime degree l, F being an algebraic function field over a finite field of constants. The formula giving the number of ambiguous classes plays a key role in this evaluation. Knowing the ramification, one can calculate the ambiguous class number from this formula, except in the case when the lth roots of unity are contained in the field of constants and the degrees of all the ramified primes are divisible by l. In this case the least positive degree of an invariant divisor class is 1 or l. Both the possibilities are realized. This answers affirmatively a question of Rosen [5].

2. Galois Cohomology

Let E/k be a cyclic extension of prime degree l of an algebraic function field F/k having the finite field k as its exact field of constants. We use the following notation:

$D_E\,(D_{0E})$	the group of divisors (of degree 0) of E
$C_E\,(C_{0E})$	the group of divisor classes (of degree 0) of E
$I_E\,(I_{0E})$	the group of idéles (of degree 0) of E
$J_E\,(J_{0E})$	the group of idéle classes (of degree 0) of E
P_E	the group of principal divisors of E
t	the number of ramified primes
$\delta_{(E/F)}$	the gcd of l and the degrees of the ramified primes
$\bar{c}$	the minimal positive degree of an invariant divisor class
$G = \mathrm{gal}(E/F)$	
$h^i(G, M)$	the order of the cohomology group $H^i(G, M)$.

We use the same symbol to denote a field and its multiplicative group. Finally, for a G-module M, M^G will denote the submodule of invariant elements.

We evaluate the cohomology groups for the various G-modules that are associated with the extension E/F. In particular, we prove

Theorem 1 (a) *If E/F is unramified,*

$$h^0(G, C_{0E}) = h^1(G, C_{0E}) = h^0(G, C_E)$$
$$= lh^1(G, C_E) = l^2 \quad \text{if } k \text{ contains the } l\text{th roots of unity;}$$
$$= l \quad \text{if } k \text{ does not contain the } l\text{th roots of unity.}$$

(b) *If E/F is ramified,*

$$h^0(G, C_{0E}) = h^1(G, C_{0E}) = \delta(E/F)l^t \quad \text{if } k \text{ does not contain the } l\text{th roots of unity;}$$

$$= l^{t-1} \quad \text{if } k \text{ contains the } l\text{th roots of unity and } \delta(E/F) = 1;$$

$$= \bar{c}l^t \quad \text{if } k \text{ contains the } l\text{th roots of unity and } \delta(E/F) = l;$$

$$h^0(G, C_E) = lh^1(G, C_E) = l^t \quad \text{if } k \text{ contains the } l\text{th roots of unity and } \delta(E/F) = 1;$$

$$= l^{t+1} \quad \text{otherwise.}$$

Proof Since G is cyclic, $H^i(G, M) \cong H^{i+2}(G, M)$. Further, if the module is finite, by Herbrand's lemma, $h^i(G, M) = h^{i+1}(G, M)$. Thus,

$$h^1(G, C_{0E}) = h^0(G, C_{0E}) = [C_{0E}^G : \mathrm{Norm}(C_{0E})]$$
$$= [C_{0E}^G : C'_{0F}][C'_{0F} : \mathrm{Norm}(C_{0E})], \tag{1}$$

C'_{0F} denoting the image of C_{0F} under the canonical conorm map $C_{0F} \to C_{0E}$ induced by the inclusion $F \subset E$.

We have the ambiguous class number formula [6]

$$\bar{h}_E = [C_{0E}^G : 1] = \frac{h_F \cdot \bar{c} \cdot l^t \cdot [\bar{\eta} : \eta]}{a[\varepsilon : 1]} \tag{2}$$

where $h_F = [C_{0F} : 1]$ is the class number of F; a the minimal positive degree in E of a divisor of F; $\bar{\eta}$ the elements in the multiplicative group of k that are norms from E; η the elements of k that are norms of units of E; and ε the kernel of the norm map restricted to the units.

We also know [2]

$$[C'_{0F} : 1] = \frac{h_F}{l} \quad \text{if } E/F \text{ is unramified and } k \text{ contains the } l\text{th roots of unity;}$$

$$= h_F \quad \text{otherwise.} \tag{3}$$

From (2) and (3), we can calculate $[C_{0E}^G : C'_{0F}]$.

To evaluate the second factor on the right-hand side in (1), consider the canonical exact sequence of G-modules

$$1 \to E \to I_E \to J_E \to 1.$$

In cohomology, it gives the exact sequence

$$1 \to E^G = F \to I_E^G = J_E^G \to H^1(G, E).$$

The group $H^1(G, E)$ is trivial by Hilbert's Theorem 90. Therefore, every invariant idèle class contains an invariant idèle. Also, it follows from definition that

$$I_E^G = I_F, \qquad I_{0E}^G = I_{0F}.$$

Thus,

$$J_E^G = J_F, \qquad J_{0E}^G = J_{0F}.$$

Consider the canonical map

$$J_{0E} \to C_{0E}.$$

Restricted to J_{0E}^G, it gives the epimorphism

$$J_{0E}^G = J_{0F} \to C'_{0F}.$$

Norms correspond to norms. Therefore,

$$h^0(G, J_{0E}) = [J_{0E}^G\text{: norms}] = [C'_{0F}\text{: norm}(C_{0E})]. \tag{4}$$

Considering the rational integers Z as a G-module under trivial action, we have the exact sequence of G-modules

$$1 \to J_{0E} \to J_E \xrightarrow{\text{degree}} Z \to 0. \tag{5}$$

We are using here F. K. Schmidt's theorem [7] which states that for finite k the algebraic function field has a divisor of degree one. From (5), we obtain, in cohomology, the exact sequence

$$H^{-1}(G, Z) \to H^0(G, J_{0E}) \to H^0(G, J_E) \xrightarrow{\rho} H^0(G, Z) \to H^1(G, J_{0E}) \to H^1(G, J_E). \tag{6}$$

From class field theory, $H^1(G, J_E)$ is trivial and $H^0(G, J_E)$ has order l. Also,

$$H^{-1}(G, Z) \cong H^1(G, Z) \cong \frac{\text{crossed homomorphisms}}{\text{principal crossed homomorphisms}} = 1$$

$$H^0(G, Z) \cong \frac{\text{invariant elements}}{\text{norms}} \cong \frac{Z}{lZ}.$$

Idèle classes of F have their degrees multiplied by l when considered as idèle classes of E. Therefore, the map ρ in (6) is the zero map. Hence,

$$h^0(G, J_{0E}) = h^0(G, J_E) = h^1(G, J_{0E}) = l. \tag{7}$$

From (1), (4), (7), (2), and (3), we have

$$h^0(G, C_{0E}) = l[C_{0E}^G : C'_{0F}]$$
$$= l^2(\bar{h}_E/h_F) \quad \text{if } E/F \text{ is unramified and } k \text{ contains the } l\text{th roots of unity;}$$
$$= l(\bar{h}_E/h_F) \quad \text{otherwise.} \tag{8}$$

As mentioned above, the degree of a divisor of F gets multiplied by l when considered as a divisor of E. Therefore, by F. K. Schmidt's theorem, $a = l$ in (2). From (2) and (8), we have

$$h^0(G, C_{0E}) = \bar{c}[\bar{\eta} : \eta] \quad \text{if } E/F \text{ is unramified and } k \text{ contains the } l\text{th roots of unity;}$$
$$= \frac{\bar{c}l^t[\bar{\eta} : \eta]}{[\varepsilon : 1]} \quad \text{otherwise.} \tag{9}$$

We separate, now, the ramified and the unramified cases.

E/F Unramified Let $\bar{E}/\bar{F}$ be the extension obtained by making a constant extension of degree l. Let $\Gamma = \text{gal}(\bar{E}/E) = \text{gal}(\bar{F}/F)$. As in [2], consider the exact sequence of Γ-modules, induced by the inclusion $\bar{F} \subset \bar{E}$,

$$1 \to \bar{N} \to C_{0\bar{F}} \to C'_{0\bar{F}} \to 1.$$

In cohomology, it gives

$$1 \to \bar{N}^\Gamma \to C_{0\bar{F}}^\Gamma \to (C'_{0\bar{F}})^\Gamma \to H^1(\Gamma, \bar{N}) \to H^1(\Gamma, C_{0\bar{F}}).$$

If k contains the lth roots of unity,

$$l = (\bar{N})^\Gamma = \bar{N}, \qquad C_{0\bar{F}}^\Gamma = C_{0F}, \qquad h^1(\Gamma, C_{0\bar{F}}) = 1, \qquad h^1(\Gamma, \bar{N}) = l.$$

Therefore, $h_F = [(C'_{0\bar{F}})^\Gamma : 1]$. If k does not contain the lth roots of unity, then $\bar{N} = 1$ and the last equation is still valid.

Clearly, $(C'_{0\bar{F}})^\Gamma \subset C_{0E}^G$. Therefore,

$$h_F | \bar{h}_F. \tag{10}$$

For an unramified extension, every unit is a norm. If k does not contain the lth roots of unity, this is trivial because, then, every unit is norm of a unit. If k contains the lth roots of unity, this is a result of class field theory. Thus, in each case,

$$\frac{[\bar{\eta} : \eta]}{[\varepsilon : 1]} = 1. \tag{11}$$

From (2), (10), and (11),

$$\bar{c} = l, \qquad \bar{h}_E = h_F . \tag{12}$$

Substitution in (8) or (9) gives

$$h^0(G, C_{0E}) = h^1(G, C_{0E}) = l^2 \quad \text{if } k \text{ contains the } l\text{th roots of unity;}$$
$$= l \quad \text{otherwise.} \tag{13}$$

To calculate $h^0(G, C_E)$ and $h^1(G, C_E)$, consider the exact sequence of G-modules

$$1 \to C_{0E} \to C_E \xrightarrow{\text{degree}} Z \to 0. \tag{14}$$

In cohomology, (14) gives

$$1 \to C_{0E}^G \to C_E^G \xrightarrow{\mu} Z \to H^1(G, C_{0E}) \to H^1(G, C_E) \to 1. \tag{15}$$

By (12), the image under μ is lZ. Therefore, (13) and (15) imply, if k contains the lth roots of unity,

$$h^1(G, C_{0E}) = l^2 = lh^1(G, C_E). \tag{16}$$

By Herbrand's lemma,

$$\frac{h^0(G, C_E)}{h^1(G, C_E)} = \frac{h^0(G, Z)}{h^1(G, Z)} \times \frac{h^0(G, C_{0E})}{h^1(G, C_{0E})} = \frac{h^0(G, Z)}{h^1(G, Z)} = l.$$

Therefore, (16) gives

$$h^0(G, C_E) = l^2. \tag{17}$$

Similarly,

$$h^1(G, C_E) = 1, \qquad h^0(G, C_E) = l \tag{18}$$

if k does not contain the lth roots of unity.

Before we study the ramified case, we evaluate $H^1(G, P_E)$ in general. To that end, consider the exact sequence

$$1 \to k \to E \to P_E \to 1,$$

obtaining in cohomology

$$H^{-1}(G, E) = 1 \to H^{-1}(G, P_E) \to H^0(G, k) \xrightarrow{\lambda} H^0(G, E) \to \cdots.$$

Therefore, $h^{-1}(G, P_E) =$ order of the kernel of λ. If k does not contain the lth roots of unity, $h^0(G, k) = 1$. If k contains the lth roots of unity, $h^0(G, k) = l$.

In this case a generator of k is a norm from E iff it is everywhere locally a norm iff the degrees of the ramified primes are all divisible by l. This follows from Hasse's norm theorem. Therefore,

$$h^{-1}(G, P_E) = h^1(G, P_E) = l \quad \text{if } k \text{ contains the } l\text{th roots of unity and the degrees of the ramified primes are all divisible by } l;$$

$$= 1 \quad \text{otherwise.} \tag{19}$$

E/F Ramified We assert that

$$\bar{c} = \delta(E/F)$$

$$= \text{the minimal positive degree of an invariant divisor,} \tag{20}$$

if k does not contain the lth roots of unity. For, consider the exact sequence

$$1 \to P_E \to D_E \to C_E \to 1,$$

and the induced cohomology sequence

$$1 \to P_E^G \to D_E^G \to C_E^G \to H^1(G, P_E) \to \cdots \tag{21}$$

(19) and (21) imply that every invariant class contains an invariant divisor. Therefore, $\bar{c} = \delta(E/F)$. Substitution in (9) gives

$$h^0(G, C_{0E}) = \delta(E/F)l^t \quad \text{if } k \text{ does not contain the } l\text{th roots of unity;}$$

$$= l^{t-1} \quad \text{if } k \text{ contains the } l\text{th roots of unity and } \delta(E/F) = 1;$$

$$= \bar{c}l^t \quad \text{if } k \text{ contains the } l\text{th roots of unity and } \delta(E/F) = l. \tag{22}$$

The orders $h^0(G, C_E)$ and $h^1(G, C_E)$ are calculated, as in the unramified case, by considering the exact sequence (14). The values are

$$h^0(G, C_E) = lh^1(G, C_E) = l^t \quad \text{if } k \text{ contains the } l\text{th roots of unity and } \delta(E/F) = 1;$$

$$= l^{t+1} \quad \text{otherwise.} \tag{23}$$

From (13), (16), (17), (22), and (23), we see that proof of Theorem 1 is complete.

We observe that it is only the last case in (22) that involves $\bar{c}$. Rosen [5] asked the question if $\bar{c} = 1$ can, at all, occur in this case. An affirmative answer is provided by the following.

Proposition *Let characteristic $k \neq 2$ and $P(x)$ be an irreducible monic polynomial of degree $4n + 2$ in $k[x]$. Then $E = k(x)(\sqrt{p(x)})$ contains an invariant class of degree one.*

Proof Consider the quadratic constant extension $\bar{E}$. The polynomial $p(x)$ decomposes as the product of two monic irreducible polynomials over the extended field of constants. The formula (2) for the ambiguous class number shows that the class number of $\bar{E}$ is odd. Since $\mathrm{gal}(\bar{E}/E)$ operates on $C_{0\bar{E}}$ and C_{0E} is the invariant subgroup, it follows that h_E is also odd. Now, the ambiguous class number formula applied to E shows that it has an invariant class of degree one.

Remark 1 Some of the arguments used in the proof of Theorem 1 also appear in Rosen's paper [5]. We have repeated them here to make this paper self-contained.

Remark 2 It was proved [2] that h_F divides h_E if E/F is a normal extension. Rosen [5] gave another proof. We observe that the normality is an unnecessary restriction. Using some results from the theory of abelian varieties, one can, in fact, show that the quotient of the zeta functions is a polynomial with rational integral coefficients. To give an arithmetic proof for $h_F \mid h_E$, one can assume that there is no field strictly between F and E, and that the canonical map $C_{0F} \to C_{0E}$ has a nontrivial kernel. This implies that E/F is a pure extension of degree l, a prime. The proof [2] for the divisibility is valid in this case. If E/F is nonnormal, a proof can also be given by considering a Hilbert class field H of F, i.e., a maximal abelian unramified extension of F that has k as its exact field of constants. Then, $H \cap E = F$ and EH/E is abelian and unramified. A simple argument shows that k is the exact field of constants of HE. Therefore, by the reciprocity law, C_{0F} is a subgroup of C_{0E}.

3. A Theorem of E. Artin

Let k be a finite field and $k(x)$ be the field of rational functions in one indeterminate. Following Artin, we call a quadratic extension $E/k(x)$ imaginary if the infinite prime of $k(x)$ does not split in E. Let R be the integral closure of $k[x]$ in E. Then, R is a Dedekind domain with finite class group. There are only finitely many imaginary quadratic extensions $E/k(x)$ for which the class group of R has exponent 2. We wish to obtain bounds on the genus of such fields. We shall assume that the genus $g_E = g > 1$ and, hence [4], $|k| \doteq q \leq 5$.

If h_x is the class number of R, one has the relation [7]

$$h_x = f h_E , \tag{24}$$

where $f = 1$ or 2 according as the infinite prime ramifies or is inert. In each case, C_{0E} is a subgroup of the class group of R. Therefore, its exponent is also 2. (We leave out of consideration the 5 fields [3] for which $h_E = 1$.) Now, C_{0E} has exponent 2 iff it is equal to its subgroup of ambiguous classes, i.e.,

$$h_E = \bar{h}_E = \bar{c} \times 2^{t-1} \times \frac{[\bar{\eta}: \eta]}{[\varepsilon: 1]} = 2^d. \tag{25}$$

Let m be any natural number not less than $2g - 1$. Then, by the Riemann–Roch theorem, the dimension of a class of degree m is $m - g + 1$. The total number of integral divisors in all the classes of degree m is

$$2^d(q^{m-g+1} - 1)(q - 1)^{-1}.$$

Also, by the Riemann hypothesis, the constant extension of degree m has, at least, $q^{m/2}(q^{m/2} - 2g)$ primes of degree one. Considering that a prime of E of degree dividing m can give, at most, m primes of degree one in the constant extension, we see that E has, at least, $m^{-1}q^{m/2}(q^{m/2} - 2g)$ integral divisors of degree m. Therefore, the exponent of C_{0E} is larger than 2 if

$$(q - 1)q^{m/2}(q^{m/2} - 2g) > m2^d(q^{m-g+1} - 1). \tag{26}$$

We consider the two cases when the characteristic is even and when it is odd.

Case 1 *characteristic* $= 2$ In this case, (20) and (25) give

$$h_E = \bar{h}_E = 2^d = \bar{c}2^{t-1} = \delta(E/k(x))2^{t-1}. \tag{27}$$

The genus formula gives $2g + 2 = D$, D denoting the degree of the different. We observe that the ramification being wild, a ramified prime of degree s makes a contribution of, at least, $2s$ to D.

Consider the case when $q = 2$ and no prime of degree one ramifies. For $g = 9$, (28) gives $2^d \leq 2^3$. Substituting $m = 2g - 1$, $d = 3$ in (26), we verify that the inequality is satisfied. We omit the formal argument showing that (26) is satisfied for all $g \geq 9$. It is not satisfied for $g = 8$.

When $q = 4$ and no prime of degree one ramifies, one sees, similarly, that (26) is always satisfied.

If $q = 4$ or 2 and a prime of degree one ramifies, Madden [4] has shown that $g \leq 2$, $g \leq 4$, respectively. These bounds are better than those derived from (26).

Case 2 *characteristic different from* 2 Consider the case when no prime of degree one ramifies. By (26) and [1],

$$\begin{aligned} h_x = 2h_E &= 2^t \quad \text{if} \quad \delta(E/k(x)) = 2 \\ &= 2^{t-1} \quad \text{if} \quad \delta(E/k(x)) = 1. \end{aligned} \tag{28}$$

Therefore,

$$h_E = 2^d = 2^{t-1} \quad \text{if} \quad \delta(E/k(x)) = 2$$
$$= 2^{t-2} \quad \text{if} \quad \delta(E/k(x)) = 1. \tag{29}$$

In this case, the ramification is tame. A ramified prime of degree s makes a contribution of, at least, s to D. Taking $m = 2g - 1$, one can show that (26) is satisfied for $q = 3$ and 5 if $g \geq 5$, $g \geq 2$, respectively. For example, if $q = 3$, $g = 5$, then $D = 12$. This implies $t \leq 5$. Therefore, from (29), $d \leq 4$, in each case. Substituting in (26) shows that it is satisfied.

If a prime of degree one ramifies, Madden's estimates are better. Combining our results with those of Madden, we have

Theorem 2 *Let $E/k(x)$ be an imaginary quadratic extension such that the integral closure of $k[x]$ in E has class group of exponent 2. Then, the null class group of E also has exponent 2. The various possibilities are*

$$q = 7, 9, \qquad g = 1;$$
$$q = 4, 5, \qquad g \leq 2;$$
$$q = 3, \qquad g \leq 4;$$
$$q = 2, \qquad g \leq 8.$$

If no prime of degree one ramifies, $g = 2$ is not possible for $q = 4$ and 5.

REFERENCES

[1] E. Artin, Quadratische Körper im Gebiete der höheren Kongruenzen, I und II, *Math. Z.* **19** (1924).
[2] M. Madan, On class numbers in fields of algebraic functions, *Arch. Math. (Basel)* **21** (1970).
[3] M. Madan and C. Queen, Algebraic function fields of class number one, *Acta Arith.* **20** (1972).
[4] D. Madden, Quadratic function fields with invariant class group, *J. Number Theory* (to appear).
[5] M. Rosen, Ambiguous divisor classes in function fields, *J. Number Theory* (to appear).
[6] M. Moriya, Rein arithmetisch-algebraischer Aufbau der Klassenkörpertheorie über algebraischen Funktionenkörpern einer Unbestimmten mit endlichem Konstantenkörper, *Japan J. Math.* **15** (1938).
[7] F. K. Schmidt, Analytische Zahlentheorie in Körpern der Charakteristik p, *Math. Z.* **33** (1931).

AMS (MOS) 1970 subject classification: 12A60.

On Some Special Decimal Fractions

K. MAHLER

AUSTRALIAN NATIONAL UNIVERSITY
CANBERRA, AUSTRALIA

For a special countable set of irrational numbers, infinitely many integral multiples are constructed the decimal expansions of which begin with very large numbers of the digit 9.

Real irrational numbers have the well-known property that the fractional parts of their multiples lie dense, and even are uniformly distributed, between 0 and 1. In a different direction I recently proved [2] the following result: To every positive integer n there exists a second positive integer $P = P(n)$ such that, if α is any real irrational number, then there is a positive integer $p = p(\alpha, n)$ satisfying $1 \leq p \leq P(n)$ such that every possible sequence of n digits 0, 1, 2, ..., 9 occurs infinitely often in the decimal expansion of $p\alpha$.

In the present note, I shall establish a result of a somewhat different kind. Let $f(x)$ be a positive integral valued polynomial of degree $m \geq 1$, and let $\sigma(f)$ be the decimal fraction obtained by writing the decimal forms of $f(1)$, $f(2), f(3), \ldots$ successively after the decimal point. *Then, for every sufficiently large positive integer N, among the first $10^{N/m}$ digits after the decimal point of*

$$((10^1 - 1)(10^2 - 1) \cdots (10^N - 1))^{m+1}\sigma,$$

there are at most $(m + 1)N^3$ digits distinct from 9.

Almost forty years ago I had studied these numbers [1] and proved that they are transcendental, but are not Liouville numbers. In the present note I apply both notations and results of this old paper.

1.

We begin with an almost trivial lemma.

Lemma *Let*

$$\sigma = r_0 - \sum_{\nu=1}^{\infty} r_\nu \cdot 10^{-i_\nu}$$

be a convergent series where the r_ν are positive rational numbers, and the i_ν are strictly increasing positive integers. Denote by d_N a common denominator of r_0, $r_1, \ldots, r_N$, and by e_N and ε_N positive integers such that

$$d_N \cdot \max(r_0, r_1, \ldots, r_N) < 10^{e_N}, \qquad d_N \cdot \sum_{\nu=N+1}^{\infty} r_\nu 10^{-i_\nu} < 10^{-\varepsilon_N}.$$

If

$$\varepsilon_N > Ne_N,$$

then at least $\varepsilon_N - Ne_N$ of the first ε_N digits after the decimal point in the decimal expansion of $d_N\sigma$ are equal to 9.

Proof The positive integer $d_N r_0$ can be written as

$$d_N r_0 = (d_N r_0 - 1) + 0.999 \ldots,$$

where the decimal fraction has only digits 9. Hence

$$d_N\sigma = (d_N r_0 - 1) + 0.999 \ldots - \sum_{\nu=1}^{N} d_N r_\nu \cdot 10^{-i_\nu} - d_N \cdot \sum_{\nu=N+1}^{\infty} r_\nu \cdot 10^{i_\nu}.$$

Here, by the definition of e_ν and ε_ν, each of the decimal representations for the integers $d_N r_1, d_N r_2, \ldots, d_N r_N$ contains at most e_N digits distinct from 0, and the decimal expansion of the convergent series

$$d_N \cdot \sum_{\nu=N+1}^{\infty} r_\nu \cdot 10^{-i_\nu}$$

has only zero digits in the first ε_N places after the decimal point. On account of the term 0.999 ... the assertion follows immediately.

2.

The numbers $\sigma(f)$ of my paper [1] were defined as follows. Denote by $f(x)$ a polynomial of the exact degree $m \geq 1$ which for positive integral x

assumes only nonnegative integral values and write

$$f_h(x) = \Delta^h f(x) = \sum_{H=0}^{h} (-1)^H \binom{h}{H} f(x + h - H) \qquad (h = 0, 1, 2, \ldots)$$

for the successive differences of $f(x)$. We need consider these differences only for $0 \leq h \leq m$ because those with $h \geq m + 1$ vanish identically. All these differences have integral values for all positive integers x, and they are moreover positive if x is sufficiently large.

Without loss of generality, we impose the stronger restriction that $f(x)$ is strictly increasing and positive for $x \geq 1$ and that moreover

$$f_h(x) > 0 \qquad \text{for} \quad 0 \leq h \leq m \text{ and } x \geq 1.$$

It follows in particular that, for $y \geq f(1) \geq 1$, there exists the inverse function $x = g(y)$ of $y = f(x)$, and here also $g(y)$ is strictly increasing.

A little more can be said. We can write $f(x)$ in the explicit form

$$f(x) = \alpha^{-m} x^m (1 + \alpha_1 x^{-1} + \alpha_2 x^{-2} + \cdots + \alpha_m x^{-m}),$$

where α is a certain positive number and $\alpha_1, \alpha_2, \ldots, \alpha_m$ are certain real constants. Hence it follows that for sufficiently large y,

$$g(y) = \alpha y^{1/m} + O(1). \tag{1}$$

3.

For every positive integer k the function value $f(k)$ can be written as a finite decimal

$$f(k) = \sum_{\lambda=0}^{M_k} d_{k\lambda} 10^{M_k - \lambda} = d_{k0} d_{k1} \cdots d_{kM_k},$$

where the coefficients $d_{k\lambda}$ are decimal digits 0, 1, ..., 9, where in particular

$$d_{k0} > 0 \qquad \text{for all } k,$$

and where the numbers M_k are nondecreasing nonnegative integers.

We associate now with the polynomial $f(x)$ the infinite decimal fraction

$$\sigma(f) = 0 \cdot d_{10} d_{11} \cdots d_{1M_1} d_{20} d_{21} \cdots d_{2M_2} d_{30} d_{31} \cdots d_{M_3} \cdots.$$

By way of example, the polynomial

$$\phi(x) = x(x + 1)/2$$

has the required properties, and with it is associated the decimal fraction

$$\sigma(\phi) = 0.1\ 3\ 6\ 10\ 15\ 21\ 28\ 36\ 45\ 55\ 66\ 78\ 91\ 105\ 120\ 136 \ldots.$$

From my old paper [1] I take a strongly convergent series for $\sigma(f)$. Denote by n the positive integer for which

$$10^{n-1} \leq f(1) \leq 10^n - 1,$$

and put

$$j_{n-1} = 0 \quad \text{and} \quad j_\nu = [g(10^\nu - 1)] \qquad \text{for} \quad \nu = n, n+1, n+2, \ldots;$$

further write

$$J_\nu = \sum_{\mu=n}^{\nu-1} \mu(j_\mu - j_{\mu-1}) = (\nu-1)j_{\nu-1} - \sum_{\mu=n}^{\nu-2} j_\mu$$

$$\text{for} \quad \nu = n+1, n+2, n+3, \ldots.$$

With this notation

$$\sigma(f) = \sum_{k=1}^{j_n} f(k)10^{-kn} + \sum_{\nu=n+1}^{\infty} 10^{-J_\nu + j_{\nu-1}} \sum_{k=j_{\nu-1}+1}^{j_\nu} f(k)10^{-k\nu}.$$

Here the finite sums can be summed by means of a formula from difference calculus, giving the formula

$$\sigma(f) = \sum_{h=0}^{m} f_h(1)(10^n - 1)^{-(h+1)}$$

$$- \sum_{\nu=n+1}^{\infty} 10^{-J_\nu} \sum_{h=0}^{m} f_h(j_{\nu-1}+1)((10^{\nu-1}-1)^{-(h+1)} - (10^\nu - 1)^{-(h+1)}). \tag{2}$$

4.

On putting

$$r_0 = \sum_{h=0}^{m} f_h(1)(10^n - 1)^{-(h+1)},$$

$$r_{\nu-n} = \sum_{h=0}^{m} f_h(j_{\nu-1}+1)((10^{\nu-1}-1)^{-(h+1)} - (10^\nu - 1)^{-(h+1)})$$

$$\text{for} \quad \nu \geq n+1,$$

$$i_\nu = J_{n+\nu} \qquad \text{for} \quad \nu \geq 1,$$

the formula (2) can be written as

$$\sigma(f) = r_0 - \sum_{\nu=1}^{\infty} r_\nu 10^{-i_\nu}, \tag{3}$$

a series of the same form as in the lemma. From their definitions, all the numbers $r_0, r_1, r_2, \ldots$ are positive and rational. The coefficients $f_h(1)$ and $f_h(j_{\nu-1}+1)$ are positive integers. If further d_N denotes the product

$$d_N = ((10^1-1)(10^2-1)\cdots(10^N-1))^{m+1}, \tag{4}$$

then d_N is a common denominator of the $N+1$ rational numbers $r_0, r_1, \ldots, r_N$, and

$$d_N < (10^{1+2+\cdots+N})^{m+1} = 10^{(m+1)N(N+1)/2}.$$

In order to make use of the lemma, we require upper estimates for the numbers e_ν and ε_ν. Such estimates can be derived from the formula (1) for $g(y)$. It implies that for large ν

$$j_\nu = \alpha \cdot 10^{\nu/m} + O(1) \qquad \text{and} \qquad J_\nu = \alpha(\nu-1)\cdot 10^{(\nu-1)/m} + O(10^{(\nu-1)/m}), \tag{5}$$

This implies that there are two positive constants c and C such that for large ν,

$$c\nu \cdot 10^{\nu/m} \le i_\nu \le C\nu \cdot 10^{\nu/m}. \tag{6}$$

Further, for $h = 0, 1, \ldots, m$, and for large x,

$$f_h(x) = O(x^m),$$

hence, by (5), for all such values of h and for large ν,

$$f_h(j_{\nu-1}+1) = O(10^\nu).$$

On the other hand, for such h and ν,

$$(10^{\nu-1}-1)^{-(h+1)} - (10^\nu - 1)^{-(h+1)} = O(10^{-\nu}).$$

Therefore all the sums $r_0, r_1, r_2, \ldots$ are bounded positive numbers, say not larger than $10^p - 1$ where p is some positive integer. This means that for sufficiently large integers N the products $d_N r_0, d_N r_1, d_N r_2, \ldots$ are positive integers not greater than

$$10^{(m+1)N^2} - 1,$$

therefore by (6) that

$$0 < \sum_{\nu=N+1}^{\infty} d_N r_\nu \cdot 10^{-i_\nu} < 10^{-10^{N/m}}.$$

The hypothesis of the lemma is thus satisfied with

$$e_N = (m+1)N^2 \qquad \text{and} \qquad \varepsilon_N = 10^{N/m}.$$

Here $\varepsilon_N > Ne_N$ for all sufficiently large N, and hence the lemma leads to the following result.

Theorem *The decimal fraction $\sigma(f)$ belonging to a polynomial $f(x)$ of degree m has the following property. To every sufficiently large positive integer N there exists a positive integer d_N of at most $(m+1)N(N+1)/2$ decimal places such that at least $10^{N/m} - (m+1)N^3$ of the first $10^{N/m}$ digits after the decimal point in the decimal expansion of $d_N\sigma(f)$ are equal to 9.*

REFERENCES

[1] Kurt Mahler, Arithmetische Eigenschaften einer Klasse von Dezimalbrüchen, *Proc. Akad. Wetenschappen, Amsterdam* **40** (1937), 421–428.

[2] Kurt Mahler, Arithmetical properties of the digits of the multiples of an irrational number, *Bull. Austral. Math. Soc.* **8** (1973), 191–203.

Sums from a Sequence of Group Elements

JOHN E. OLSON *EDWARD T. WHITE*

THE PENNSYLVANIA STATE UNIVERSITY
UNIVERSITY PARK, PENNSYLVANIA

The following theorem is proved. If $g_1, g_2, \ldots, g_k$ is a sequence of elements from a group (written additively) such that $\langle g_1, g_2, \ldots, g_k \rangle$ is not cyclic, then either the set of all sums $g_{i_1} + g_{i_2} + \cdots + g_{i_t}$ $(1 \le i_1 < i_2 < \cdots < i_t \le k;\ t \ge 1)$ contains 0, or it contains at least $2k - 1$ elements.

1. Introduction

Given a sequence of elements $g_1, \ldots, g_k$ (possibly with repetition) in a group G (written additively), we shall say that the sequence *represents* g if g occurs as a sum of the form

$$g = g_{i_1} + \cdots + g_{i_t} \qquad (1 \le i_1 < \cdots < i_t \le k; \quad t \ge 1).$$

For finite Abelian groups, the problem of determining the length of the longest sequence in the group that does not represent 0 has been extensively studied [1–3, 6], and, though solved for Abelian p-groups and for a number of other cases, remains unsolved in the general case. Much less is known for non-Abelian groups. In this paper we shall prove the following result for an arbitrary group.

Theorem *If the sequence $g_1, \ldots, g_k$ does not represent* 0, *and if the group*

$\langle g_1, \ldots, g_k \rangle$ generated by the g_i is not cyclic, then the sequence does represent at least $2k - 1$ elements.

From this theorem we shall obtain the

Corollary *If G is a finite, but noncyclic group of order n, then every sequence in G of length $k \geq \frac{1}{2}(n + 1)$ represents 0.*

The corollary was proved for Abelian groups by R. B. Eggleton and P. Erdös [4]. In the same paper, Eggleton and Erdös proved that any sequence of k *distinct* elements in an Abelian group, which does not represent 0, does represent at least $2k - 1$ elements.

It is interesting to note that our theorem and corollary give the best possible results in the case of dihedral groups, and that this is so even if we take sequences of distinct elements. To see this, let G be the (dihedral) group of order $n = 2v$ generated by a and b, where $2a = 0$, $vb = 0$, and $b + a = a - b$. For $k \leq v$, form the sequence

$$a, \quad a + b, \quad a + 2b, \quad \ldots, \quad a + (k - 1)b.$$

It is easy to see that this sequence represents exactly $2k - 1$ elements, namely

$$a, \quad a + b, \quad \ldots, \quad a + (k - 1)b; \quad b, \quad 2b, \quad \ldots, \quad (k - 1)b.$$

More generally, the theorem gives, for a given k, the best possible result in any noncyclic group G that has an element x of order at least k. For if $y \in G$, but $y \notin \langle x \rangle$, the sequence

$$x, \ldots, x, y \qquad \text{(where } x \text{ is repeated } k - 1 \text{ times)}$$

does not represent 0 and does represent exactly $2k - 1$ elements.

2. Notation and Preliminaries

If A and B are nonempty subsets of a group G, take $A + B$ to be the set of all elements of the form $a + b$ with $a \in A$, $b \in B$. The notation $|X|$ will signify the number of elements in a finite set X. If $a_1, \ldots, a_k$ are nonzero group elements, the symbol $\Sigma = \Sigma(a_1, \ldots, a_k)$ will always denote the sum set

$$\Sigma = \{0, a_1\} + \{0, a_2\} + \cdots + \{0, a_k\},$$

that is, the set of all elements $\varepsilon_1 a_1 + \cdots + \varepsilon_k a_k$, where $\varepsilon_i = 0$ or 1. Thus $0 \in \Sigma$. If $\varepsilon_1 a_1 + \cdots + \varepsilon_k a_k = 0$ ($\varepsilon_i = 0$ or 1) has no solution other than $\varepsilon_1 = \cdots = \varepsilon_k = 0$, we shall say that 0 has only the *trivial representation* in Σ. By a *coset* of a subgroup H we shall always mean a right coset $H + g$. If Σ contains an element of a coset $H + g$, we shall say that Σ *represents* that coset.

We shall require the following lemmas:

Lemma 1 *If 0 has only the trivial representation in* $\Sigma = \Sigma(a_1, \ldots, a_k)$, *then* $|\Sigma| \geq k + 1$ *and equality holds only when* $a_1 = a_2 = \cdots = a_k$.

Proof The lemma is easy to verify for $k = 1, 2$. Assume that $k \geq 3$ and that the lemma is true for sequences of length $k - 1$. Since 0 has only the trivial representation, $0 \notin a_1 + \Sigma(a_2, \ldots, a_k)$. Therefore $|\Sigma| \geq 1 + |\Sigma(a_2, \ldots, a_k)|$. The lemma follows, by induction, from this inequality except when $a_2 = a_3 = \cdots = a_k$ and $a_1 \neq a_2$. But, by symmetry, $|\Sigma| \geq 1 + |\Sigma(a_1, \ldots, a_{k-1})|$. Hence, in the remaining case, $|\Sigma| \geq k + 2$.

Lemma 2 *Suppose* $\langle a \rangle$ *is a cyclic group of order n and* $S = \{0, a, 2a, \ldots, ta\}$, *where* $0 \leq t \leq n - 2$. *If* $0 \neq h \in \langle a \rangle$, *then* $|S + \{0, h\}| \geq t + 2$.

Proof If h lies in S, then $-a + h \in S$, but $-a + h \notin S + h$. If not, then $h \in S + h$ but $h \notin S$. Thus, in any case, $S \neq S + h$. Since $S + \{0, h\} = S \cup S + h$, we have $|S + \{0, h\}| > |S| = t + 1$.

Lemma 3 *Suppose* $\langle a \rangle$ *is a cyclic group of odd order n and* $S = \{0, a, 2a, \ldots, ta\}$, *where* $2 \leq t \leq n - 1$. *If* $h \in \langle a \rangle$, *h is not a generator of* $\langle a \rangle$, *and* $0 \notin S + h$, *then* $|S + \{0, h\}| \geq t + 4$.

Proof Since $\langle a \rangle$ has odd order and h is not a generator, $h \neq a, 2a$. Also $h \neq 0$ since h is in $S + h$ but 0 is not. Thus $h = ra$, where $3 \leq r \leq n - 1$. Since $S + h = \{ra, (r + 1)a, \ldots, (r + t)a\}$ and $0 \notin S + h$, we must have $r + t \leq n - 1$. Hence 0, a, and $2a$ are not in $S + h$. Since these three elements are in S, it follows that $|S + \{0, h\}| \geq |S + h| + 3 = |S| + 3 = t + 4$.

Lemma 4 (Kemperman) *Suppose A and B are finite subsets of a group and* $0 \in A \cap B$. *If* $a + b = 0$ $(a \in A, b \in B)$ *has no solution except* $a = b = 0$, *then* $|A + B| \geq |A| + |B| - 1$.

The proof of this lemma may be found in Kemperman [5].

3. Proof of the Theorem

Assume that the theorem is false and let $a_1, \ldots, a_k$ be a criminal sequence of minimal length k. Thus $\langle a_1, \ldots, a_k \rangle$ is not cyclic, $|\Sigma(a_1, \ldots, a_k)| < 2k$ and 0 has only the trivial representation in $\Sigma(a_1, \ldots, a_k)$. Let $H = \langle a_1, \ldots, a_t \rangle$, where t is the largest index such that $\langle a_1, \ldots, a_t \rangle$ is cyclic. We may assume that our sequence is chosen, from among the criminal sequences of length k, to have maximal value t. Let u be the largest integer such that $\langle a_{k-u+1}, \ldots,$

$a_k\rangle$ is cyclic. Under these assumptions we first show

Lemma 5 *Let* $\Sigma = \Sigma(a_1, \ldots, a_k)$.

(a) $|\Sigma| = 2k - 1$, $|\Sigma(a_1, \ldots, a_{k-1})| = |\Sigma(a_2, \ldots, a_k)| = 2k - 2$.
(b) $H + \Sigma = \Sigma$.
(c) *H is a finite subgroup of odd order.*
(d) *Σ is the union of at least three cosets of H.*
(e) $u \leq t \leq k - 4$ *and* $t \leq |H| - 2$.

Proof We must have $a_1 \in \langle a_2, \ldots, a_k\rangle$, for otherwise $a_1 + \Sigma(a_2, \ldots, a_k)$ and $\Sigma(a_2, \ldots, a_k)$ are disjoint sets, and so $|\Sigma| \geq 2|\Sigma(a_2, \ldots, a_k)|$. But this is impossible since, by Lemma 1, $|\Sigma(a_2, \ldots, a_k)| \geq k$. It follows, in particular, that $\langle a_2, \ldots, a_k\rangle$ is not cyclic. Thus, by the minimality of k, $|\Sigma(a_2, \ldots, a_k)| \geq 2k - 2$. Since 0 has only the trivial representation in Σ, $0 \notin a_1 + \Sigma(a_2, \ldots, a_k)$. This shows that $|\Sigma| \geq 1 + |\Sigma(a_2, \ldots, a_k)|$. Thus equality must hold in the last two inequalities. Similarly $|\Sigma(a_1, \ldots, a_{k-1})| = 2k - 2$. This proves (a).

Since $|\Sigma| = 1 + |\Sigma(a_2, \ldots, a_k)|$ and $0 \notin a_1 + \Sigma(a_2, \ldots, a_k)$, we must have that $\Sigma = \{0\} \cup a_1 + \Sigma(a_2, \ldots, a_k)$. Thus if $x \in \Sigma$ and $x \neq 0$, then $-a_1 + x \in \Sigma(a_2, \ldots, a_k)$. In particular

$$x \in \Sigma, \qquad x \neq 0 \rightarrow -a_1 + x \in \Sigma. \tag{1}$$

Similarly,

$$x \in \Sigma, \qquad x \neq 0 \rightarrow x - a_k \in \Sigma. \tag{2}$$

From (1) it follows that if $x \in \Sigma$ but $x \notin \langle a_1\rangle$, then x, $-a_1 + x$, $-2a_1 + x$, ... all lie in Σ. Since Σ does contain elements not in $\langle a_1\rangle$, we see that a_1 has finite order. Hence

$$x \in \Sigma, \qquad x \notin \langle a_1\rangle \rightarrow \langle a_1\rangle + x \subseteq \Sigma. \tag{3}$$

We shall show that the restriction "$x \neq 0$" in (1) can be eliminated, or, in other words, $-a_1 \in \Sigma$. To do this we need to know that $a_1 \neq a_k$. We shall show that $a_k \notin \langle a_1\rangle$. Suppose, to the contrary, $a_k \in \langle a_1\rangle$. Consider the sequence $a_k, a_1, a_2, \ldots, a_{k-1}$. Clearly 0 has only the trivial representation in $\Sigma(a_k, a_1, a_2, \ldots, a_{k-1})$. Let $y \in \Sigma(a_1, \ldots, a_{k-1})$. If $y \in \langle a_1\rangle$, then a_k and y commute, so $a_k + y = y + a_k \in \Sigma$. If $y \notin \langle a_1\rangle$, then, by (3), $\langle a_1\rangle + y \subseteq \Sigma$, so $a_k + y \in \Sigma$. This proves that $\Sigma(a_k, a_1, \ldots, a_{k-1}) \subseteq \Sigma$. Therefore $a_k, a_1, \ldots, a_{k-1}$ is a criminal sequence of length k and $\langle a_k, a_1, \ldots, a_t\rangle$ is cyclic. But this contradicts the maximality of t. Thus $a_k \notin \langle a_1\rangle$.

By (1), $-a_1 + a_k \in \Sigma$. Since $a_1 \neq a_k$, we have, by (2), that $(-a_1 + a_k) - a_k \in \Sigma$. Thus $-a_1 \in \Sigma$. Thus (1) becomes: $x \in \Sigma \rightarrow -a_1 + x \in \Sigma$. This gives

$$\langle a_1\rangle + \Sigma = \Sigma. \tag{4}$$

Since the elements $a_1, \ldots, a_t$ commute, we may interchange a_1 with any a_j

$(j = 2, \ldots, t)$, so (4) holds with a_1 replaced by a_j. Thus $\langle a_j \rangle + \Sigma = \Sigma$ for all $j = 1, \ldots, t$. It follows that

$$H + \Sigma = \Sigma. \tag{5}$$

We see, by (5), that H is finite and that Σ is the union of complete cosets of H. Hence $|\Sigma| = |H|m$, where m is the number of cosets of H represented by Σ. By (a), $|\Sigma|$ is odd, hence $|H|$ and m are odd. But $m > 1$, so $m \geq 3$. This proves (b), (c), and (d).

Clearly $-a_k, \ldots, -a_2, -a_1$ is a criminal sequence, so, by the maximality of t, $t \geq u$. By Lemma 1, $|\Sigma(a_1, \ldots, a_t)| \geq t + 1$. Thus $t + 1 \leq |H|$. If $t = |H| - 1$, then, by Lemma 1, $\Sigma(a_1, \ldots, a_t) = H$. But this means that $H + \Sigma(a_1, \ldots, a_j) = \Sigma(a_1, \ldots, a_j)$, for all $t \leq j \leq k$. Hence $|H|$ divides $|\Sigma(a_1, \ldots, a_j)|$ for all $t \leq j \leq k$. But this is impossible since $t < k$, $|\Sigma(a_1, \ldots, a_{k-1})| = 2k - 2$, and $|\Sigma| = 2k - 1$. Thus $t \leq |H| - 2$.

Since $2k - 1 = |\Sigma| \geq 3|H| \geq 3t + 6$, we have $k \geq t + 4$. This completes the proof of (e) and the lemma.

Lemma 6 *Either* (i) *there is an index* s *such that*

$$|\Sigma(a_1, \ldots, a_s)| \geq 2s + t, \tag{6}$$

or (ii) $t = 1$ *and* $a_2 = a_3 = a_4$.

Proof By Lemma 5, Σ represents at least three cosets of H. Let v be the smallest index such that $\Sigma(a_1, \ldots, a_v)$ represents three (or more) cosets of H. Thus $v \geq t + 2$. Let $S = \Sigma(a_1, \ldots, a_t)$. If $w \in \Sigma(a_{t+1}, \ldots, a_v)$, then $S + w \subseteq \Sigma(a_1, \ldots, a_v)$. Thus $\Sigma(a_1, \ldots, a_v)$ contains at least $|S|$ elements in each coset it represents. Since $\Sigma(a_1, \ldots, a_v)$ represents at least one more coset than $\Sigma(a_1, \ldots, a_{v-1})$, we have

$$|\Sigma(a_1, \ldots, a_v)| \geq |\Sigma(a_1, \ldots, a_{v-1})| + |S| \geq 2v - 2 + |S|.$$

By Lemma 1, $|S| \geq t + 1$. If $|S| \geq t + 2$, we are done. Also we are done if $\Sigma(a_1, \ldots, a_v)$ represents four or more cosets of H, for then

$$|\Sigma(a_1, \ldots, a_v)| \geq 2v - 2 + 2|S| \geq 2v - 2 + 2(t + 1) > 2v + t.$$

By Lemma 1, $|S| = t + 1$ only when $a_1 = a_2 = \cdots = a_t$.

Thus we may assume that $a_1 = a_2 = \cdots = a_t = a$, hence $S = \{0, a, 2a, \ldots, ta\}$, and that $\Sigma(a_1, \ldots, a_v)$ represents exactly three cosets of H.

Let $x = a_{t+1}$. By the meaning of v, $\Sigma(a_1, \ldots, a_{v-1}) \subseteq H \cup H + x$. Thus we may write $\Sigma(a_1, \ldots, a_{v-1}) = A \cup B + x$, where $S \subseteq A$, $B \subseteq H$. The third coset represented by $\Sigma(a_1, \ldots, a_v)$, but not by $\Sigma(a_1, \ldots, a_{v-1})$, is either $H + a_v$ or $H + x + a_v$. Thus if $|A| \geq t + 2$ and $|B| \geq t + 2$, we are done and (6) holds with $s = v$. For notational convenience, we shall label the first $t + 3$ elements of our sequence (recall $k \geq t + 4$ by Lemma 5) as $a, \ldots, a, x, y, z$. We consider five cases.

Case 1 $v \geq t+4$ In this case $\Sigma(x, y, z) \subseteq H \cup H + x$. Since the three elements y, z, and $y + z$ lie in $H \cup H + x$, at least one of them lies in H. Label that element h_1. Clearly $h_1 \neq 0$. Thus $x + h_1 \in \Sigma(x, y, z)$. Now $x + h_1$ is not in H, hence $x + h_1 = h_2 + x$, where $0 \neq h_2 \in H$. Thus $A \supseteq S + \{0, h_1\}$ and $B \supseteq S + \{0, h_2\}$. By Lemma 5, $t \leq |H| - 2$, hence Lemma 2 gives $|A|$, $|B| \geq t + 2$.

Case 2 $v = t + 3$ and $x \neq y$ Thus $\Sigma(a, \ldots, a, x, y) = A \cup B + x$. Since $x \notin H$, we have $H + x + y \neq H + y$. Thus one of $x + y$ and y lies in H and the other lies in $H + x$. Since neither is 0 or x, they have the form h_1, $h_2 + x$, where $h_1, h_2 \neq 0$ and $h_1, h_2 \in H$. Thus $A \supseteq S + \{0, h_1\}$ and $B \supseteq S + \{0, h_2\}$. Again $|A|$, $|B| \geq t + 2$, by Lemma 2.

Case 3 $v = t + 2$ and $x \neq y$ The four elements $0, x, y, x + y$ are distinct, and $\Sigma(a, \ldots, a, x, y)$ represents exactly three cosets of H, hence some two of these four elements lie in the same coset of H. Thus $\Sigma(x, y)$ contains two elements of the form $w, h + w$, where $0 \neq h \in H$. By Lemma 2, $|S + \{0, h\}| \geq t + 2$, hence at least $t + 2$ elements of $\Sigma(a, \ldots, a, x, y)$ lie in $H + w$. Since the other two cosets each contain at least $t + 1$ elements of $\Sigma(a, \ldots, a, x, y)$, we have $|\Sigma(a, \ldots, a, x, y)| \geq 3t + 4 = 2v + t$. Thus (6) holds with $s = v$.

Case 4 $v = t + 3$ and $x = y$ In this case $x + y = 2x = h$ lies in H and $h \neq 0$. Since $\langle a, \ldots, a, x \rangle$ is not cyclic, h is not a generator of $H = \langle a \rangle$. Also $0 \notin S + h$ since 0 has only the trivial representation in Σ.

If $t > 1$, then (since H has odd order, by Lemma 5) Lemma 3 applies, and we have $|S + \{0, h\}| \geq t + 4$. Hence $|\Sigma(a, \ldots, a, x, y, z)| \geq 3t + 6 = 2v + t$, and so (6) holds with $s = v$.

If $t = 1$, then $A = S + \{0, h\} = \{0, a, a + h, h\}$, and $|A| = 4$, since $h \neq 0, \pm a$. If $z \notin H$, then $|A \cup A + z| \geq 8$, and so $|\Sigma(a, x, y, z)| \geq 10$. If $z \in H$, then $0 \notin A + z$, since 0 has only the trivial representation; therefore $|A + \{0, z\}| \geq |A| + 1 = 5$. Thus $\Sigma(a, x, y, z)$ contains five elements of H, and so $|\Sigma(a, x, y, z)| \geq 9$. Thus in either case (6) holds with $s = v = 4$.

Case 5 $v = t + 2$ and $x = y$ Thus $\Sigma(a, \ldots, a, x, x) = S \cup S + x \cup S + 2x$, where 0, x, and $2x$ are in different cosets of H. If $\Sigma(x, x, z)$ represents five or more cosets of H, then $|\Sigma(a, \ldots, a, x, x, z)| \geq 5(t + 1) > 2(v + 1) + t$. If $\Sigma(x, x, z)$ represents four cosets of H and $t > 1$, then $|\Sigma(a, \ldots, a, x, x, z)| \geq 4(t + 1) \geq 2(v + 1) + t$. So, in either of these two cases, we may take $s = v + 1$ in (6).

Assume $t = 1$ and $\Sigma(a, x, x, z)$ represents exactly four cosets of H. We may assume that $z \neq x$, for otherwise statement (ii) of the lemma holds. Since $z \neq x$, $\Sigma(x, x, z)$ contains at least five elements by Lemma 1. Hence two elements of $\Sigma(x, x, z)$ lie in the same coset of H. Thus $w, h + w \in \Sigma(x, x, z)$, where $0 \neq h \in H$. Since a has odd order, $S + \{0, h\} = \{0, a, h, a + h\}$ contains at least three elements. Thus $H + w$ intersects

$\Sigma(a, x, x, z)$ in at least three elements. It follows that $|\Sigma(a, x, x, z)| \geq 3 + 2 + 2 + 2 = 9$, hence (6) holds with $s = v + 1 = 4$.

There remains only the possibility that $\Sigma(a, \ldots, a, x, x, z)$ represents exactly three cosets of H. Thus the three cosets $H + z$, $H + x + z$, $H + 2x + z$ coincide, possibly in different order, with $H, H + x, H + 2x$. If $S + ix + z \neq S + jx$ for all $0 \leq i, j \leq 2$, then each coset $H + ix$ $(i = 0, 1, 2)$ intersects $\Sigma(a, \ldots, a, x, x, z)$ in at least $|S| + 1 = t + 2$ elements, and so $|\Sigma(a, \ldots, a, x, x, z)| \geq 3t + 6 = 2(t + 3) + t$, which means that (6) holds with $s = t + 3 = v + 1$. Assume that $S + ix + z = S + jx$ for some pair i, j $(0 \leq i, j \leq 2)$. Then $S = S + (ix + z - jx)$. Then by Lemma 2, $ix + z - jx = 0$, so $z = (j - i)x$. Since the three elements z, $x + z$, and $x + x + z$ cannot be zero, we must have $z = x$ or $z = 2x$. In either case $3x \in \Sigma(x, x, z)$, $3x = h \in H$, $0 \notin S + h$, and, since $\langle a, x \rangle$ is not cyclic, h is not a generator of H.

If $t > 1$, then, by Lemma 3, $|S + \{0, h\}| \geq t + 4$. Hence H intersects $\Sigma(a, \ldots, a, x, x, z)$ in at least $t + 4$ elements, and therefore $|\Sigma(a, \ldots, a, x, x, z)| \geq 3t + 6 = 2(t + 3) + t$. Thus (6) holds with $s = t + 3 = v + 1$.

If $t = 1$, we may assume $z \neq x$ (otherwise (ii) holds), so $z = 2x$. Then by Lemma 1, $|\Sigma(x, x, 2x)| \geq 5$. But $a \notin \langle x \rangle$, so $a + \Sigma(x, x, 2x)$ and $\Sigma(x, x, 2x)$ are disjoint. Thus $|\Sigma(a, x, x, 2x)| \geq 2|\Sigma(x, x, 2x)| \geq 10$, and again (6) holds with $s = 4 = v + 1$. This completes the proof of the lemma.

It is now easy to obtain a contradiction from all of this. Suppose first that statement (i) of Lemma 6 holds. Thus there is an index s for which $|\Sigma(a_1, \ldots, a_s)| \geq 2s + t$. We may assume, of course, that $s < k$, thus $\Sigma = \Sigma(a_1, \ldots, a_s) + \Sigma(a_{s+1}, \ldots, a_k)$. Since 0 has only the trivial representation in Σ, 0 has only the trivial representation as a sum $0 = a + b$, $a \in \Sigma(a_1, \ldots, a_s)$, $b \in \Sigma(a_{s+1}, \ldots, a_k)$. Thus, by Lemma 4,

$$|\Sigma| \geq |\Sigma(a_1, \ldots, a_s)| + |\Sigma(a_{s+1}, \ldots, a_k)| - 1.$$

If $\langle a_{s+1}, \ldots, a_k \rangle$ is not cyclic, we have $|\Sigma(a_{s+1}, \ldots, a_k)| \geq 2(k - s)$, hence $|\Sigma| \geq 2k + t - 1 \geq 2k$, and we are done. If $\langle a_{s+1}, \ldots, a_k \rangle$ is cyclic, then, by the definition of u, $k - s \leq u$. Also $|\Sigma(a_{s+1}, \ldots, a_k)| \geq k - s + 1$, by Lemma 1. Thus $|\Sigma| \geq s + k + t \geq 2k + t - u \geq 2k$ and we are done.

Suppose that statement (ii) of Lemma 6 holds. Thus $t = 1$ and $a_2 = a_3 = a_4$. Let r be the largest integer such that $\langle a_2, a_3, \ldots, a_{r+1} \rangle = Q$ is cyclic. Thus $r \geq 3$. Also $r + 1 < k$ since $u = 1$.

We first show that $\Sigma(a_2, \ldots, a_k)$ represents at least three cosets of Q. The elements $0, a_1 + a_2, -a_1 + a_2$ lie in Σ, by (b) of Lemma 5. By (a) of Lemma 5, there is only one element in Σ that is not in $\Sigma(a_2, \ldots, a_k)$. This element must be $-a_1$ since $-a_1 \in \Sigma$ by (b) of Lemma 5, and since $-a_1 \notin \Sigma(a_2, \ldots, a_k)$ since 0 has only the trivial representation in Σ. Now $0, a_1 + a_2, -a_1 + a_2$ are distinct from $-a_1$ since a_1 has odd order and $a_1 \notin Q$. Thus 0,

$a_1 + a_2$, $-a_1 + a_2 \in \Sigma(a_2, \ldots, a_k)$. Therefore $\Sigma(a_2, \ldots, a_k)$ represents the three cosets Q, $Q + a_1 + a_2$, $Q - a_1 + a_2$, which are distinct, again since a_1 has odd order and $a_1 \notin Q$.

Let $v + 1$ be the largest index such that $\Sigma(a_2, \ldots, a_{v+1})$ represents three or more cosets of Q. Since $a_2 = a_3 = a_4 \in Q$ and $|\Sigma(a_2, a_3, a_4)| \geq 4$, every coset of Q represented by $\Sigma(a_2, \ldots, a_{v+1})$ intersects $\Sigma(a_2, \ldots, a_{v+1})$ in at least four elements. Thus $|\Sigma(a_2, \ldots, a_{v+1})| \geq 4 + |\Sigma(a_2, \ldots, a_v)|$. Since $v > r + 1$, $\langle a_2, \ldots, a_v \rangle$ is not cyclic, hence $|\Sigma(a_2, \ldots, a_v)| \geq 2(v - 1)$, and so $|\Sigma(a_2, \ldots, a_{v+1})| \geq 2(v + 1)$. By Lemma 5, $|\Sigma(a_2, \ldots, a_k)| = 2k - 2$, so $v + 1 < k$. Lemma 4 gives

$$|\Sigma(a_2, \ldots, a_k)| \geq 2v + 1 + |\Sigma(a_{v+2}, \ldots, a_k)|.$$

If $\langle a_{v+2}, \ldots, a_k \rangle$ is not cyclic, then $|\Sigma(a_{v+2}, \ldots, a_k)| \geq 2(k - v - 1)$, and hence $|\Sigma(a_2, \ldots, a_k)| \geq 2k - 1$, which is a contradiction. If $\langle a_{v+2}, \ldots, a_k \rangle$ is cyclic, then $k - v - 1 = u = 1$ and so $|\Sigma(a_2, \ldots, a_k)| \geq 2k - 1$, which is again a contradiction. This completes the proof of the theorem.

To prove the corollary, suppose $a_1, \ldots, a_k$ is a sequence in a noncyclic group G of order n, and $k \geq \frac{1}{2}(n + 1)$. If the sequence does not represent 0, then $|\Sigma(a_1, \ldots, a_k)| \geq k + 1 > n/2$ by Lemma 1. Hence $\langle a_1, \ldots, a_k \rangle = G$. But then, by the theorem, $|\Sigma(a_1, \ldots, a_k)| \geq 2k > n$, which is impossible.

REFERENCES

[1] P. C. Baayen, "Een combinatorisch probleem voor eindige Abelse groepen." Math. Centrum Syllabus 5, Colloquium Discrete Wiskunde Caput 3. Math. Centre Amsterdam, 1968.

[2] P. van Emde Boas, A combinatorial problem on finite Abelian groups, II, Rep. ZW-1969-007. Math. Centre Amsterdam (1969).

[3] P. van Emde Boas and D. Kruyswijk, A combinatorial problem on finite Abelian groups, III, Rep. ZW-1969-008. Math. Centre Amsterdam (1969).

[4] R. B. Eggleton and P. Erdös, Two combinatorial problems in group theory, *Acta Arith.* **21** (1972), 111–116.

[5] J. H. B. Kemperman, On complexes in a semigroup, *Indag. Math.* **18** (1956), 247–254.

[6] J. E. Olson, A combinatorial problem on finite Abelian groups, I and II, *J. Number Theory* **1** (1969), 8–10 and 195–199.

AMS (MOS) 1970 subject classifications: 20F50, 05A05.

Concerning a Possible "Thue–Siegel–Roth Theorem" for Algebraic Differential Equations

CHARLES F. OSGOOD

NAVAL RESEARCH LABORATORY
WASHINGTON, D.C.

Let K denote a field of characteristic zero. Let y_1 denote a formal power series about $z = \infty$ with coefficients in K which is a solution of a nonzero algebraic differential equation having its coefficients in K. Let ord *denote order of vanishing at $z = \infty$. We show that for each $\varepsilon > 0$ there exist a constant $c(\varepsilon) > 0$ and a nonzero algebraic differential equation A_ε, having coefficients in K, such that for all $r, s \not\equiv 0$ in $K[z]$ either,* (i) $\operatorname{ord}(y_1 - rs^{-1}) \leq (2 + \varepsilon) \deg s$, (ii) $\deg s < c(\varepsilon)$, *or* (iii) *rs^{-1} is a solution of A_ε. In a number of cases both $c(\varepsilon)$ and A_ε are effectively computable. If one could eliminate case* (iii), *a very strong statement of approximation would follow, a statement analogous in many ways to the Thue–Siegel–Roth theorem. Inequality* (i) *is best possible in the sense that, as one may easily show, given any formal series y_1 with* ord $y_1 = 0$ *and any positive integer n there exist polynomials r and s, with* $\deg s \leq n$, *such that* $\operatorname{ord}(sy - r) > n \geq \deg s$. *(Consider the rank of the associated system of linear homogeneous equations.)*

Introduction

Kolchin, in [2], suggested the problem of proving an analogue of the Thue–Siegel–Roth theorem for (at least) all formal power series y_1, with coefficients in a field K of characteristic zero, that satisfy an algebraic differential equation. He obtained what may be thought of as a "Liouville type" of

bound on the "diophantine approximation" of such formal series by rational functions. In two recent papers [3, 4] the present author used the methods of differential equations in order to obtain effective bounds on the "diophantine approximation" of algebraic functions over fields K of *both* zero and positive characteristic. The present results represent a considerable generalization of the methods used by Osgood [3] and Osgood [4]. We obtain below an incomplete solution to the Kolchin problem, as we understand it and have interest in it; i.e., for each power series y_1 and every $\varepsilon > 0$, our analogue of the Thue–Siegel–Roth theorem holds, for all rational functions *not* satisfying a certain algebraic differential equation, $P_\varepsilon = 0$. Here $P_\varepsilon \not\equiv 0$ is a differential polynomial depending upon both the differential equation satisfied by y_1 and upon ε. In many cases P_ε is effectively computable.

Since our method could be used to construct a number of (potentially) distinct differential polynomials P_ε, one would hope that future work in this area might show† (sometimes even effectively) that beyond some point the only common zeros of all of these differential polynomials P_ε are the solutions to our original algebraic differential equation for y_1. Then if, say, y_1 is not a singular solution of our original differential equation for it (which we shall have to assume below anyway) the argument of Kolchin in [2] would suffice to complete a (noneffective) proof of our analogue of the Thue–Siegel–Roth theorem. The effective approach used in [3] by the present author might then even allow one to obtain this latter result effectively, in certain cases.

Finally, the approach of this paper can be carried out in more general contexts. In particular, in Theorem II below, we consider what can be shown over an arbitrary differential field of characteristic zero. We have no interest here in other valuations than ord. Extensions to other valuations are likely. (Presumably, with minor changes, the proof would also go through for fields of positive characteristic. This is of less interest, perhaps, since there exist algebraic differential equations, such as $y^{(p)} = 0$, which have in their solution set every formal power series with coefficients in any field of characteristic $p > 0$.)

1.

Definitions Let K denote a field of characteristic zero. Let z be transcendental over K. Let A denote a nonzero algebraic differential equation over K, i.e., A is of the form $\alpha(y, y^{(1)}, \ldots, y^{(n)}, z) = 0$ where each

† (February 1976) As stated, this now appears unlikely to me; however, it would be enough to show that y_1 is not a limit point (in ord) of the set of *common* zeros of all of these differential polynomials.

$y^{(j)} = (d/dz)^j y$, $0 \le j < \infty$, n is a nonnegative integer, and $\alpha(y, y^{(1)}, \ldots, y^{(n)}, z)$ is a not identically zero polynomial in $n + 2$ variables with coefficients in K. Let y_1 denote a (generalized) formal power series solution of A about $z = \infty$, i.e.,

$$y_1 = \sum_{l=0}^{\infty} a_l z^{-l+m}$$

for some integer m and a set of elements a_l in K. Suppose that y_1 is not a solution of $\partial\alpha/\partial y^{(n)} = 0$. Let ord f denote, for any formal power series f about $z = \infty$, the order of vanishing of f at $z = \infty$.

Theorem I (i) *For each $\varepsilon > 0$ there exist a nonzero algebraic differential equation A_ε with coefficients in K and a positive constant $c(\varepsilon)$ such that*

$$\operatorname{ord}(y_1 - rs^{-1}) < (2 + \varepsilon) \deg s \tag{1}$$

for all polynomials r and $s \neq 0$, in z, with coefficients in K, such that rs^{-1} is not a solution of A_ε, and deg $s \ge c(\varepsilon)$.

(ii) *If K equals the rational field, then A_ε is effectively computable, and if we know, in addition, a lower bound on* ord y_1, *then $c(\varepsilon)$ is also effectively computable.*

The following theorem strengthens Theorem I in a rather surprising manner.

Theorem I′ *Suppose, under the hypotheses of Theorem* I, *that additionally* ord $y_1 \ge 0$, *then Theorem* I *holds (for a potentially different A_ε) with $c(\varepsilon) \equiv 1$. If $K = Q$, the rational field, and if there exists an effective algorithm for deciding if y_1 satisfies a given algebraic differential equation with coefficients in Q, then our new A_ε is effectively computable.*

(To handle the general case multiply y_1 above by z^{-M}, where $-M \le$ ord y_1, and apply Theorem I′ to $z^{-M}y_1$, where it is being approximated by $z^{-M}rs^{-1}$.)

Theorem I′ holds out the (remote) possibility that the constructions in the present paper might someday be used to prove an inequality of the form $\operatorname{ord}(y_1 - rs^{-1}) < 2(\deg s) + \eta(y_1)$, for some $\eta(y_1) > 0$ and with no exceptions, *since one may now choose $\varepsilon > 0$ after a specific rs^{-1}* has been chosen. *On the other hand, if* deg $s \ge 1$, *and we choose $\varepsilon < (\deg s)^{-1}$*, then (1) *would be false infinitely often (see the abstract). The (hopefully not usual) case that rs^{-1} satisfies A_ε is forced upon us under these circumstances.*

Theorems I and I′ will follow easily from a more general result:

Definitions Let F denote a differential field, of zero characteristic with derivation δ. (For these definitions, see Kolchin [1].) By a nonzero differential polynomial P over F, we mean an expression of the form $P(y, y^{(1)}, \ldots,$

$y^{(n)}$) where y is a differential indeterminate (see Kolchin [1] again) $y^{(j)} = \delta^j y$, $0 \leq j < \infty$, the parameter n is a nonnegative integer, and $P(y, y^{(1)}, \ldots, y^{(n)})$ is a polynomial in $n + 1$ variables over F. (The extension of this definition to more than one differential indeterminate is straightforward.)

By the "denomination" of a differential polynomial $P = P(y, y^{(1)}, \ldots, y^{(n)})$ over F we shall mean the smallest nonnegative integer $d = d(P)$ such that $y^d P(wy^{-1}, \ldots, (wy^{-1})^{(n)})$ is a differential polynomial in the two differential indeterminates w and y. By the principal differential ideal (in $F[y, y^{(1)}, \ldots, y^{(j)}, \ldots]$) generated by a differential polynomial we shall mean the smallest (algebraic) ideal in $F[y, \ldots, y^{(j)}, \ldots]$ that both contains α and is closed under differentiation (as we shall refer to the action of the derivation). We denote this ideal as (α). Similarly, if our ring is $F[y, y^{(1)}, \ldots; X_1, X_1^{(1)}, \ldots; \ldots; X_n, X_n^{(1)}, \ldots]$ where $y, X_1, \ldots, X_n$ are distinct differential indeterminates, we denote the corresponding ideal as $(\alpha)F[X_1, \ldots, X_n]$.

Theorem II (i) *For each nonzero differential polynomial $\alpha = \alpha(y, \ldots, y^{(n)})$, with $\partial\alpha/\partial y^{(n)} \not\equiv 0$, and each $\varepsilon > 0$, there exists a positive integer φ, a nonzero differential polynomial $P_\varepsilon \in F[y, y^{(1)}, \ldots]$, and a real number $\theta_\varepsilon \geq 1$ satisfying $d(P_\varepsilon)\theta_\varepsilon^{-1} < 2 + \varepsilon$, such that each*

$$\left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^{\varphi}\left[\left(\frac{\partial}{\partial y}\right)^{e_0}\left(\frac{\partial}{\partial y^{(1)}}\right)^{e_1}\cdots\left(\frac{\partial}{\partial y^{(j)}}\right)^{e_j}\cdots\right]P_\varepsilon \in (\alpha)$$

for all sequences of nonnegative integers $e_0, e_1, \ldots$ with $\sum_j e_j < \theta_\varepsilon$.

(ii) *Further, one may effectively compute P_ε if F is the field of rational functions in one variable with rational (number) coefficients.*

2.

We wish to see that Theorem I follows from Theorem II. By Theorem II, given $\varepsilon > 0$ there exists (or we may effectively compute) a differential polynomial $P_{\varepsilon/2}$ such that each

$$\left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^{\varphi}\left[\left(\frac{\partial}{\partial y}\right)^{e_0}\cdots\left(\frac{\partial}{\partial y^{(j)}}\right)^{e_j}\cdots\right]P_{\varepsilon/2} \in (\alpha)$$

if $\sum_j e_j < \theta_{\varepsilon/2}$, where $\theta_{\varepsilon/2}$ is such that $d(P_{\varepsilon/2})(\theta_{\varepsilon/2})^{-1} < 2 + \varepsilon/2$. Then we see that the (finite) Taylor series expansion of $P_{\varepsilon/2}$ in powers of $(y - y_1)$, $(y - y_1)^{(1)}, \ldots$ has zero coefficients for all terms of total degree less than $\theta_{\varepsilon/2}$ in $(y - y_1), (y - y_1)^{(1)}, \ldots$. Let A_ε be $P_{\varepsilon/2} = 0$. If

$$P_{\varepsilon/2}((r/s), (r/s)^{(1)}, \ldots) \neq 0$$

then, since ord of a nonzero rational function is at most the degree of the

denominator,

$$\text{ord } P_{\varepsilon/2}(r/s, (r/s)^{(1)}, \ldots) \leq d(P_{\varepsilon/2}) \deg s.$$

Suppose $\text{ord}(r/s - y_1) > 0$ and

$$\text{ord}(r/s - y_1) \geq (2 + \varepsilon) \deg s > (d(P_{\varepsilon/2})(\theta_{\varepsilon/2})^{-1} + \tfrac{1}{2}\varepsilon) \deg s.$$

Then we would have that

$$\begin{aligned}\theta_{\varepsilon/2} \text{ ord}(r/s - y_1) &> d(P_{\varepsilon/2}) \deg s + \tfrac{1}{2}\varepsilon(\deg s) \\ &\geq (\text{ord } P_{\varepsilon/2}(r/s, (r/s)^{(1)}, \ldots)) + \tfrac{1}{2}\varepsilon(\deg s), \qquad (2)\end{aligned}$$

which leads to a contradiction for all s of sufficiently high degree. The bound on the degree of s depends upon a lower bound on the order of vanishing at $z = \infty$ of the coefficients of the (finite) Taylor series for $P_{\varepsilon/2}$ in $(y - y_1)$, $(y - y_1)^{(1)}, \ldots$. If $P_{\varepsilon/2}$ is effectively computable and if we can bound ord y_1 from below, we can place an effective upper bound on the degrees of those polynomials s for which there is no contradiction. This proves Theorem I, assuming Theorem II.

We shall next see that Theorem I′ also follows from Theorem II. Where $\alpha = 0$ is the original differential equation for y, suppose $\partial\alpha/\partial z \equiv 0$. Then, taking $F = K$ in Theorem II, we have $\partial P_\varepsilon/\partial z \equiv 0$. If, also, ord $y_1 \geq 0$ inequality (2), above, *now implies a contradiction regardless of the degree of s if* deg $s \geq 1$. We shall next show that there exists $\beta \not\equiv 0$ in (α) with $\partial\beta/\partial z \equiv 0$. [Since y_1 is a zero of β, obviously $\beta \notin K$. One may then proceed in our present case to take successive partial derivatives of this β, with respect to the highest derivative of y appearing in it, finally arriving at a (possibly) new $\beta = \beta(y, y^{(1)}, \ldots, y^{(m)})$ such that $\beta(y_1) = 0$ but $(\partial\beta/\partial y^{(m)})(y_1) \not\equiv 0$.] Our procedure below will be effective under the hypotheses of Theorem I′. We proceed by induction on $N = \deg_z \alpha$. If $N = 0$, there is nothing to prove. Set $\alpha = \sum_{j=0}^{N} z^j \alpha_j$, where $N \geq 1$, each $\partial\alpha_j/\partial z \equiv 0$, and $\alpha_N \not\equiv 0$. If $\alpha_N \in (\alpha)$ we have nothing to prove. If $\alpha_N \notin (\alpha)$, then $\alpha\alpha_N^{-1} \notin K$ (otherwise $\alpha_N = \alpha(\alpha_N \alpha^{-1})$ would be in (α)). Using the chain rule, we see $d(\alpha\alpha_N^{-1})/dz$ has degree in z at most $N - 1$ and is nonzero. Thus $\alpha_N^2\, d(\alpha\alpha_N^{-1})/dz \not\equiv 0$ is in (α) and has degree in z at most $N - 1$. This proves Theorem I′.

Let u, v, and y be differential indeterminates. Let ε_1 be chosen, $0 < \varepsilon_1 < 1$. *In the remainder of Section* 2 *we shall show how one may construct, for each sufficiently large positive integer* θ, *a polynomial* Q *in the* 2θ *variables* $u, u^{(1)}, \ldots, u^{(\theta-1)}, v, v^{(1)}, \ldots, v^{(\theta-1)}$, *with coefficients in* F, *having the following properties:*

(i) *The total degree of each monomial of* Q *in* $u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)}$ *is at most* 2θ.

(ii) *There exists a positive integer* φ *such that at* $v^{(j)} = (uy)^{(j)}$, $j = 0, 1, \ldots,$ *each*

$$\left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^{\varphi}\left(\frac{\partial}{\partial v}\right)^{e_0}\cdots\left(\frac{\partial}{\partial v^{(\theta-1)}}\right)^{e_{\theta-1}} Q \in (\alpha)F[u],$$

if

$$\sum_{j=0}^{\theta-1} e_j < \theta(1-\varepsilon_1).$$

Lemma I *The number of solutions in nonnegative integers of*

$$\sum_{j=1}^{\gamma} \delta_j = \beta$$

for positive integers γ *and* β *is* $\binom{\gamma+\beta-1}{\gamma-1}$. *The number of solutions of*

$$\sum_{j=1}^{\gamma} \delta_j \leq \beta$$

is $\binom{\gamma+\beta}{\gamma}$.

Proof By placing $\gamma - 1$ "cuts" in a sequence of β marks we define a unique solution above. This is equivalent to choosing $\gamma - 1$ marks out of $\gamma + \beta - 1$ marks to be "cuts." Letting $\delta_{\gamma+1}$ be

$$\beta - \sum_{j=1}^{\gamma} \delta_j$$

we see that $\binom{\gamma+\beta}{\gamma}$ is the number of solutions of

$$\sum_{j=1}^{\gamma} \delta_j \leq \beta.$$

Lemma II *If* α *has total degree* $d \geq 1$ *in* $y, y^{(1)}, \ldots, y^{(j)}, \ldots, y^{(n)}$, *where* $n \geq 0$, *then for each positive integer* θ *every*

$$\left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^{2(\theta-1)} y^{(j)}, \qquad 0 \leq j \leq \theta - 1,$$

may be written modulo (α) *as a linear combination over* F *of monomials in* $y, \ldots, y^{(n)}$, *each having total degree* $< 4\theta d$.

Proof If $j = 0, 1, \ldots, n$, there is nothing to prove. Let δ_1 denote the derivation which agrees with δ on F and is such that $\delta_1 y^{(j)} = 0, j = 0, 1, \ldots$. Now if $n + 1 \leq j < \theta$ we see that, using the chain rule $j - n$ times,

$$\Gamma_j \equiv y^{(j)} - \left(\sum_{l=0}^{n-1} y^{(l+1)}\frac{\partial}{\partial y^{(l)}} - \left[\sum_{k=0}^{n-1}\left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^{-1} y^{(k+1)}\frac{\partial\alpha}{\partial y^{(k)}} + \left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^{-1}\delta_1\alpha\right]\frac{\partial}{\partial y^{(n)}} + \delta_1\right)^{j-n} y^{(n)},$$

while not even in $F[y, y^{(1)}, \ldots, y^{(j)}, \ldots]$ is such that

$$\left(\frac{\partial \alpha}{\partial y^{(n)}}\right)^{2(j-n)-1} \Gamma_j \in (\alpha).$$

Then each

$$\left(\frac{\partial \alpha}{\partial y^{(n)}}\right)^{2(\theta-1)} y^{(j)}, \qquad 0 \leq j \leq \theta - 1,$$

may be written modulo (α) as a linear combination over F of monomials in $y, y^{(1)}, \ldots, y^{(n)}$ having total degree less than $4\theta d$. This proves Lemma II.

Using Lemmas I *and* II *we wish to see that we can construct our above-mentioned polynomial* Q. *We need to solve a system of homogeneous linear equations with coefficients in* F, *nontrivially. Therefore, we must show that we have more variables than equations. Our variables are the coefficients of the distinct differential monomials in* $u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)}$ *(potentially) appearing in* Q. *We have* $\binom{2\theta+2\theta}{2\theta} = \binom{4\theta}{2\theta}$ *such coefficients by Lemma* I. *The number of distinct monomials in* $u, \ldots, u^{(\theta-1)}$ *which we have upon setting* $v^{(k)} = (uy)^{(k)}$ *after* $0 \leq j \leq \theta(1-\varepsilon_1)$ *partial differentiations, is* $\binom{2\theta-j+\theta}{\theta} = \binom{3\theta-j}{\theta}$. *The number of distinct partial derivatives of order* $j \geq 1$ *is less than* $\binom{\theta+j}{j}$ *by Lemma* I. *Thus the total number of monomial coefficients which need to be equated to zero is at most*

$$\sum_{j=0}^{\theta(1-\varepsilon_1)} \binom{3\theta-j}{\theta}\binom{\theta+j}{j}.$$

Set $\varphi = 2\theta(2\theta-1) < 4\theta^2$ *and apply Lemma* II. *Equating each of these monomial coefficients to zero leads to at most* $\binom{n+1+8\theta^2 d}{n+1}$ *homogeneous linear equations with coefficients in* F, *using Lemma* I.

Lemma III *For all* θ *larger than some effectively computable integer,*

$$\binom{(n+1)+8\theta^2 d}{n+1} \sum_{j=0}^{\theta(1-\varepsilon_1)} \binom{3\theta-j}{\theta}\binom{\theta+j}{j} < \binom{4\theta}{2\theta}.$$

Clearly Lemma III *will suffice to show the existence of* Q. If the field F is the field of rational functions over the rational numbers, we may solve the above system of linear homogeneous equations effectively by putting the matrix of coefficients in triangular form.† Clearly a lower bound on θ may be effectively computed above in terms of ε_1 and bounds on the order of α and the degrees of α in $y, \ldots, y^{(j)}, \ldots, y^{(n)}$, for all differential fields F.

† That is, where $(a_{i,j})$ has rank n, each $a_{i,j} = 0$ if $i > n$ or $i < j$, while $a_{1,1} \cdots a_{n,n} \neq 0$.

Proof of Lemma III If θ is sufficiently large

$$\binom{(n+1)+8\theta^2 d}{n+1} < \theta^{2n+3}.$$

Now

$$\sum_{j=0}^{\theta(1-\varepsilon_1)} \binom{3\theta-j}{\theta}\binom{\theta+j}{j}$$

will be shown to be less than

$$\theta\binom{2\theta+j_1}{\theta}\binom{2\theta-j_1}{\theta},$$

where j_1 is the least integer such that $j_1 \geq \varepsilon_1 \theta$. First

$$\begin{aligned}\binom{3\theta-j}{\theta}\binom{\theta+j}{\theta} &= \binom{3\theta-(j-1)}{\theta}\binom{\theta+j-1}{\theta}\left(\frac{(2\theta-j+1)(\theta+j)}{(3\theta-j+1)j}\right)\\ &= \binom{3\theta-(j-1)}{\theta}\binom{\theta+j-1}{\theta}\left(1+\frac{2\theta(\theta+\frac{1}{2}-j)}{(3\theta-j+1)j}\right)\\ &> \binom{3\theta-(j-1)}{\theta}\binom{\theta+j-1}{\theta},\end{aligned}$$

for $j = 1, 2, \ldots, \theta$. It follows that

$$\sum_{j=1}^{\theta(1-\varepsilon_1)} \binom{3\theta-j}{\theta}\binom{\theta+j}{j} < \theta\binom{2\theta+j_1}{\theta}\binom{2\theta-j_1}{\theta}.$$

Now

$$\begin{aligned}\theta^{2n+4}\binom{2\theta+j_1}{\theta}\binom{2\theta-j_1}{\theta} &= \theta^{2n+4}\binom{2\theta}{\theta}^2 \prod_{l=0}^{\theta-1}\left\{\left(1+\frac{j_1}{2\theta-l}\right)\left(1+\frac{-j_1}{2\theta-l}\right)\right\}\\ &\leq \theta^{2n+4}\binom{2\theta}{\theta}^2 (1-j_1^2(2\theta)^{-2})^{\theta}\\ &\leq \theta^{2n+4}(1-(\tfrac{1}{2}\varepsilon_1)^2)^{\theta}\binom{2\theta}{\theta}^2.\end{aligned}$$

From the expansion of $(1+1)^{2n}$, we see that

$$2^{2n} > \binom{2n}{n} > (2n+1)^{-1}2^{2n}.$$

Thus

$$\binom{2\theta}{\theta}^2 < 2^{4\theta} < \binom{4\theta}{2\theta}(4\theta+1),$$

from which we see,

$$\theta^{2n+4}(1-(\tfrac{1}{2}\varepsilon_1)^2)^\theta\binom{2\theta}{\theta}^2 < 5\theta^{2n+5}(1-(\tfrac{1}{2}\varepsilon_1)^2)^\theta\binom{4\theta}{2\theta}.$$

Lemma III now follows.

3.

In what follows u, v, y, and Y are differential indeterminates. Now

$$Q(Yu, \ldots, (Yu)^{(\theta-1)}, Yv, \ldots, (Yv)^{(\theta-1)})$$

may be rewritten, where $e_0, \ldots, e_{\theta-1}$ are nonnegative integers, as

$$\sum_{(e_0,\ldots,e_{\theta-1})} q(e_0, \ldots, e_{\theta-1}, u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)}) \prod_{j=0}^{\theta-1} (Y^{(j)})^{e_j}.$$

Notice that at

$$v = uy, \quad \ldots, \quad v^{(\theta-1)} = (uy)^{(\theta-1)} \quad [\text{or } v = uy],$$

each

$$\left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^\varphi q(e_0, \ldots, e_{\theta-1}, u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)}) \in (\alpha)F[u]$$

since, at $v = uy$,

$$\left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^\varphi Q(Yu, \ldots, (Yu)^{(\theta-1)}, Yv, \ldots, (Yv)^{(\theta-1)}) \in (\alpha)F[Yu]$$
$$\subset (\alpha)F[u, Y].$$

Lemma IV *If*

$$\sum_{j=0}^{\theta-1} f_j < \theta(1-\varepsilon_1),$$

each

$$\left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^\varphi \times \left(\left(\frac{\partial}{\partial v}\right)^{f_0} \cdots \left(\frac{\partial}{\partial v^{(\theta-1)}}\right)^{f_{\theta-1}}\right)$$
$$\times\, q(e_0, \ldots, e_{\theta-1}, u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)}) \in (\alpha)F[u],$$

at $v = uy$.

Proof Lemma IV follows if upon applying

$$\left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^\varphi \times \left(\left(\frac{\partial}{\partial v}\right)^{f_0} \cdots \left(\frac{\partial}{\partial v^{(\theta-1)}}\right)^{f_{\theta-1}}\right)$$

to

$$Q(Yu, \ldots, (Yu)^{(\theta-1)}, Yv, \ldots, (Yv)^{(\theta-1)}),$$

and setting $v = uy$,
we obtain an element of $(\alpha)F[u, Y]$. Using the chain rule for partial differentiation, we see that what we have above is

$$\left(\frac{\partial \alpha}{\partial y^{(n)}}\right)^{\varphi} \prod_{j=0}^{\theta-1} \left(\sum_{k=0}^{\theta-1} \binom{k}{j} Y^{(k-j)} \frac{\partial}{\partial (Yv)^{(k)}}\right)^{f_j} \times Q(Yu, \ldots, (Yu)^{(\theta-1)}, Yv, \ldots, (Yv)^{(\theta-1)}).$$

This last quantity belongs to

$$(\alpha)F[u, Y] \qquad \text{at} \quad v = uy$$

since, if

$$\sum_{j=0}^{\theta-1} f_j < \theta(1 - \varepsilon_1),$$

for each choice of nonnegative integers k_j,

$$\left(\frac{\partial \alpha}{\partial y^{(n)}}\right)^{\varphi} \prod_{j=0}^{\theta-1} \left(\frac{\partial}{\partial (Yv)^{(k_j)}}\right)^{f_j} \times Q(Yu, \ldots, (Yu)^{(\theta-1)}, Yv, \ldots, (Yv)^{(\theta-1)}) \in (\alpha)F[Yu] \qquad \text{at} \quad v = uy.$$

This proves Lemma IV.

We shall next find P_ε and show that it has the desired properties—thus concluding the proof of Theorem II. From Lemma IV we see that each nonzero

$$q(e_0, \ldots, e_{\theta-1}, u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)})$$

satisfies the same hypotheses as

$$Q(u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)}).$$

Further, each is homogeneous, i.e., every monomial has the same total degree (in the derivatives of u and of v). Then, without loss of generality, we may assume in what follows that Q is homogeneous. We have either

$$Q(Yu, \ldots, (Yu)^{(\theta-1)}, (Yv), \ldots, (Yv)^{(\theta-1)}) = Y^m Q(u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)}),$$

for some nonnegative integer $m \leq 2\theta$, or there exists a *nonzero*

$$q(e_0, \ldots, e_{\theta-1}, u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)})$$

with $e_1 + \cdots + e_{\theta-1} > 0$. In the latter case replace

$$Q(u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)})$$

by a nonzero

$$q(e_0, \ldots, e_{\theta-1}, u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)})$$

with $e_1 + \cdots + e_{\theta-1} > 0$ and iterate the above argument. After at most $2\theta^2\binom{4\theta}{2\theta}$ steps (the number of differentiations occurring in our original polynomial Q is less than $2\theta^2\binom{4\theta}{2\theta}$) we must arrive at a new polynomial Q such that

$$\begin{aligned} &Q(Yu, \ldots, (Yu)^{(\theta-1)}, Yv, \ldots, (Yv)^{(\theta-1)}) \\ &\quad = Y^m Q(u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)}), \end{aligned}$$

for some nonnegative integer $m \leq 2\theta$.

Then we have

$$\begin{aligned} &Q(u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)}) \\ &\quad = u^m Q(1, 0, \ldots, 0; (v/u), \ldots, (v/u)^{(\theta-1)}). \end{aligned} \tag{3}$$

Replace v/u by y, set $\varepsilon_1 = \frac{1}{3}\varepsilon$, and set

$$Q(1, 0, \ldots, 0, y, \ldots, y^{(\theta-1)}) = P_\varepsilon(y, \ldots, y^{(\theta-1)}) = P_\varepsilon. \tag{4}$$

We must check that P_ε satisfies the conditions stated in Theorem II. Now

$$\begin{aligned} &u^m \left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^\varphi \left(\frac{\partial}{\partial y}\right)^{e_0} \cdots \left(\frac{\partial}{\partial y^{(\theta-1)}}\right)^{e_{\theta-1}} P_\varepsilon(y, \ldots, y^{(\theta-1)}) \\ &\quad = \left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^\varphi \left(\frac{\partial}{\partial y}\right)^{e_0} \cdots \left(\frac{\partial}{\partial y^{(\theta-1)}}\right)^{e_{\theta-1}} \\ &\qquad \times Q(u, \ldots, u^{(\theta-1)}, uy, \ldots, (uy)^{(\theta-1)}) \\ &\quad = \left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^\varphi \prod_{j=0}^{\theta-1} \left(\sum_{k=0}^{\theta-1} \binom{k}{j} u^{(k-j)} \frac{\partial}{\partial v^{(k)}}\right)^{e_j} \\ &\qquad \times Q(u, \ldots, u^{(\theta-1)}, v, \ldots, v^{(\theta-1)}), \end{aligned}$$

at $v = uy$. By the construction of Q the final quantity above is in $(\alpha)F[u]$ if

$$\sum_{j=0}^{\theta-1} e_j < \theta(1 - \varepsilon_1).$$

It follows that each

$$\left(\frac{\partial\alpha}{\partial y^{(n)}}\right)^\varphi \left(\frac{\partial}{\partial y}\right)^{e_0} \cdots \left(\frac{\partial}{\partial y^{(\theta-1)}}\right)^{e_{\theta-1}} P_\varepsilon(y, \ldots, y^{(\theta-1)}) \in (\alpha),$$

if $\sum_{j=0}^{\theta-1} e_j < \theta(1-\varepsilon_1)$. Notice that by (3) and (4) the denomination of P_ε, i.e., $d(P_\varepsilon)$, is at most $m \leq 2\theta$. Hence, setting $\theta_\varepsilon = \theta(1-\varepsilon_1) \geq 1$, we have (assuming without loss of generality that $0 < \varepsilon < 1$)

$$d(P_\varepsilon)\theta_\varepsilon^{-1} \leq 2(1-\varepsilon_1)^{-1} < 2 + 3\varepsilon_1 = 2 + \varepsilon.$$

If the field F equals the rational functions over the rational numbers, our construction was effective. This proves Theorem II.

REFERENCES

[1] E. R. Kolchin, "Differential Algebra and Algebraic Groups." Academic Press, New York, 1973.

[2] E. R. Kolchin, Rational approximations to solutions of algebraic differential equations, *Proc. Amer. Math. Soc.* **10** (1959), 238–244.

[3] C. F. Osgood, An effective lower bound on the "Diophantine approximation" of algebraic functions by rational functions, *Mathematika* **20** (1973), 4–15.

[4] C. F. Osgood, Effective bounds on the "Diophantine approximation" of algebraic functions over fields of arbitrary characteristic and applications to differential equations, *Proc. Koninkl Nederl. Akademie Van Wetens. Ser. A* **78** (1975), 105–119 (errata 78, No. 5).

The Minimum Discriminant of Seventh Degree Totally Real Algebraic Number Fields

M. POHST

UNIVERSITÄT KÖLN
COLOGNE, WEST GERMANY

The minimum discriminant of seventh degree totally real algebraic number fields is computed. It is 20 134 393 *and is attained only by the field* $\mathbb{Q}(\rho)$, *where* ρ *is a root of the monic irreducible polynomial* $x^7 + x^6 - 6x^5 - 5x^4 + 8x^3 + 5x^2 - 2x - 1$.

We determine the minimum discriminant essentially in the same way as J. Hunter did for quintic fields [1]. Two modifications and a fast computer enable us to handle the large number of polynomials to be considered. The modifications consist of a better bound for the polynomial coefficients (Theorem 1) and of a new method of Zassenhaus [6] for determining integral bases. Most of the underlying theory is developed by Pohst [4].

Let F be a totally real algebraic number field of degree $n = 7$. Then $F = \mathbb{Q}(\rho)$ holds, where ρ is a root of the monic irreducible polynomial

$$f(x) = x^7 + a_1 x^6 + \cdots + a_6 x + a_7 \in \mathbb{Z}[x]. \tag{1}$$

Moreover, f must have only real roots. We assume that we already know that $d_0 = 20\ 134\ 393$ is a discriminant of some field F. So we shall prove that there is no smaller discriminant d_F. In the course of our considerations it will also become clear how to obtain d_0 for a start.

We must show that there is no polynomial f the root ρ of which generates a field $F = \mathbb{Q}(\rho)$ with a discriminant $d_F < d_0$. The underlying idea is the following: If such a polynomial f exists, then there is also a polynomial $\bar{f}$ with a root $\bar{\rho}$ and $F = \mathbb{Q}(\bar{\rho})$, and the coefficients of $\bar{f}$ satisfy some inequalities $|\bar{a}_i| \leq S_i$ with suitable bounds S_i $(i = 1, \ldots, 7)$; that is, we must consider only finitely many polynomials which can be done by a computer. So at first we must derive bounds S_i which of course will depend on d_0.

Theorem I *Let F be a totally real algebraic number field of degree 7 and discriminant $d_F \leq d_0$. Then there is a generating element ρ, $F = \mathbb{Q}(\rho)$, ρ a root of a polynomial (1) with*

$$|\mathrm{tr}(\rho)| = |a_1| \leq 3, \tag{2}$$

$$\mathrm{tr}(\rho^2) \leq \tfrac{7}{4} + (\tfrac{64}{21} d_F)^{1/6} \leq \tfrac{7}{4} + (\tfrac{64}{21} d_0)^{1/6}. \tag{3}$$

From Theorem I we obtain bounds S_1, S_2, S_7 by simple calculations involving only the inequality of the arithmetic and geometric means.

$$a_1 \in \{0, 1, 2, 3\},$$

$$-\tfrac{1}{2}(\tfrac{7}{4} + (\tfrac{64}{21} d_0)^{1/6} - a_1^2) \leq a_2 \leq -\tfrac{1}{2}(8 - a_1^2),$$

$$|a_7| < ((a_1^2 - 2a_2)/7)^{7/2}, \qquad a_7 \neq 0. \tag{4}$$

Unfortunately Theorem I does not yield results for S_i with $3 \leq i \leq 6$. We get those bounds from the fact that f must have only real zeros. Then also $f^{(4)}$ has only real zeros and the discriminant of $f^{(4)}$ is positive:

$$|a_3 + \tfrac{5}{49} a_1 (2a_1^2 - 7a_2)| < \tfrac{10}{147} \sqrt{\tfrac{1}{3}(3a_1^2 - 7a_2)^3}. \tag{5}$$

Since it is difficult to compute discriminants of polynomials of degrees $n \geq 4$, we transform the property of f into a statement about a quadratic form.

Theorem II *Let $f \in \mathbb{Z}[x]$ be given as in (1). The polynomial f has only real roots if and only if the symmetric matrix $A = (a_{ij}) \in GL(6, \mathbb{Z})$ with entries*

$$a_{ij} = j(7 - i) a_i a_j - 7 \sum_{k=1}^{3} (2k + i - j) a_{i+k} a_{j-k}$$

$$(i, j = 1, \ldots, 6; \quad i \geq j; \quad a_0 = 1; \quad a_m = 0 \quad \text{if } m > 7 \text{ or } m < 0) \tag{6}$$

is positive definite. The value of the discriminant D_f of f is given by

$$D_f = 7^{-5} \det A. \tag{7}$$

Theorem II is very important for two reasons. First, we get bounds for coefficients of f from the fact that the matrix A must be positive definite, i.e., all principal minors of A must be positive. Thus the two-row principal minor

of A yields an upper bound for a_4. If $a_2 < 0$ holds, we get a lower bound for a_4 by Newton's inequalities

$$\binom{7}{i}^2 a_{i-1}a_{i+1} < \binom{7}{i-1}\binom{7}{i+1}a_i^2 \qquad (i = 1, \ldots, 6; \quad a_0 = 1). \tag{8}$$

For $a_2 = 0$ ($a_2 > 0$ does not occur), we use the fact that the discriminant of $f^{(3)}$ must be positive too:

$$a_4^3 - (\tfrac{12}{7}a_1a_3 + \tfrac{135}{343}a_1^4)a_4^2 - \tfrac{6}{49}a_1^2a_3^2a_4 - \tfrac{27}{35}a_3^4 - \tfrac{64}{343}a_1^3a_3^3 > 0. \tag{9}$$

From (9) we obtain a lower bound for a_4 by determining the smallest zero by an improved Newton's method. An inequality of Hermite provides bounds for a_5:

$$(35a_5 - 9a_1a_4 + 2a_2a_3)^2 < \tfrac{4}{5}(21a_4 - 12a_1a_3 + 5a_2^2) \times (25a_1a_5 - 20a_2a_4 + 9a_3^2). \tag{10}$$

Further, the three-row principal minor of A must be positive. This is equivalent to

$$42a_6 < 12a_3^2 - 14a_2a_4 - 28a_1a_5 + \frac{2a_{21}a_{31}a_{32} - a_{31}^2a_{22} - a_{32}^2a_{11}}{a_{11}a_{22} - a_{21}^2}. \tag{11}$$

Since the four-row principal minor of A must also be positive, we obtain an inequality $a_6^3 + r_1a_6^2 + r_2a_6 + r_3 > 0$, where the r_1, r_2, r_3 are rational numbers depending on $a_1, \ldots, a_5, a_7$. This gives us a lower bound for a_6 in the same way as for a_4. So at last we have found estimates for all coefficients of the polynomials f and must consider only finitely many of them.

The second important property of Theorem II hinges on the possibility of computing the polynomial discriminants by (7). If we compute det A by Cholesky's method, namely, we examine at the same time whether f has only real roots. Furthermore, we need the values D_f for determining the discriminants d_F of the fields F generated by some root ρ of f. D_f and d_F differ at most by a square:

$$D_f = m^2d_F \qquad (m \in \mathbb{N}), \tag{12}$$

and $D_f = d_F$ holds if and only if $1, \rho, \ldots, \rho^6$ form an integral basis of $F = \mathbb{Q}(\rho)$.

We give a short description of the corresponding computer program. It starts with seven DO-loops in which the possible polynomials f are generated as linear integer arrays $(a_1, \ldots, a_7)$. A subroutine determines the polynomial discriminants D_f. Since many discriminants are greater than 2^{31} they do not fit into one word on an IBM machine. Fortunately, all D_f are smaller than 10^{14}; we therefore carry out the calculation of D_f in double precision. Note

that Cholesky's method is numerically stable. The remaining polynomials f have only real zeros and $D_f > 0$. Then another subroutine tests whether f is irreducible. (The common algorithms are described by Knuth [2].) All reducible polynomials f are eliminated. Afterward D_f is factored into a square-free part and squares of prime numbers. Since D_f is a double precision number, this has to be done in an adequate way by an assembler subroutine. There remain 3984 polynomials f with $D_f = ab^2$ ($a, b \in \mathbb{N}$, a square-free) and $a < d_0$.

The determination of the field discriminants d_F corresponding to the D_f is carried out in three steps. Let $D_f = ab^2$ again, but a not necessarily square-free. The task is to examine whether $d_F = a < d_0$ holds.

(a) We can disprove $d_F = a$ in many cases in the following way. If $d_F = a < d_0$ holds, there would exist a generation of F in the form $F = \mathbb{Q}(\bar{\rho})$ with a smaller value of $\mathrm{tr}(\bar{\rho}^2)$ by Theorem I, i.e., there would exist a polynomial $\bar{f}, \bar{f}(\bar{\rho}) = 0$, with a greater coefficient $\bar{a}_2$ and $a \mid D_f$. This $\bar{f}$ would also be among the 3984 polynomials. If there is no such $\bar{f}$, we can eliminate f.

(b) By a method of Nagell [3] we determine the powers p^m ($m \in \mathbb{N}$) of prime numbers $p \leq 7$, $p \mid b$, which also divide d_F. Essentially we construct an integral basis of F with respect to these primes.

(c) For prime numbers p that are greater than the field degree we apply a strong method of Zassenhaus [6]. In $\mathbb{Z}[x]$ we compute the polynomials

$$D_0 = \gcd(f, f') \bmod p, \qquad C_0 = f/D_0 \bmod p,$$

$$C_1 = \gcd(f, C_0) \bmod p, \qquad D_1 = \gcd(C_0 D_0 - f, C_1) \bmod p.$$

For $D_1 = 1$ we obtain $p \nmid (D_f/d_F)$ and $D_1 \neq 1$ yields $p^2 \mid (D_f/d_F)$.

By means of these three criteria we finally get

Theorem III *The minimum discriminant of seventh degree totally real algebraic number fields is*

$$d_0 = 20\ 134\ 393 = 71 \cdot 283\ 583.$$

Remark Actually we start our computations without knowledge of d_0. Since only the lower bound for a_2 depends on d_0, we carry out the program for $a_1 \in \{0, 1, 2, 3\}$ and the corresponding greatest values for a_2 from (4). Then we proceed replacing a_2 by $a_2 - 1$ until we find a polynomial f the roots of which generate a totally real field F_1 of degree 7 and discriminant d_1. The discriminant d_1 yields a lower bound for a_2 by Theorem I. Every time we find a field of smaller discriminant we get a better lower bound for a_2. In fact d_0 is already obtained after a few steps.

It remains to show that there is—up to isomorphism—exactly one field of

discriminant d_0. Namely, we obtain 12 polynomials f with $D_f = d_0$:

$$f_1(x) = x^7 + x^6 - 6x^5 - 5x^4 + 8x^3 + 5x^2 - 2x - 1$$
$$f_2(x) = x^7 + x^6 - 6x^5 - 4x^4 + 10x^3 + 4x^2 - 4x - 1$$
$$f_3(x) = x^7 + x^6 - 8x^5 - 12x^4 + 6x^3 + 12x^2 - 1$$
$$f_4(x) = x^7 + x^6 - 10x^5 - 15x^4 + 20x^3 + 45x^2 + 18x - 1$$
$$f_5(x) = x^7 + 2x^6 - 5x^5 - 8x^4 + 5x^3 + 6x^2 - x - 1$$
$$f_6(x) = x^7 + 2x^6 - 5x^5 - 8x^4 + 8x^3 + 7x^2 - 3x - 1$$
$$f_7(x) = x^7 + 2x^6 - 6x^5 - 11x^4 + 8x^3 + 10x^2 - 4x - 1$$
$$f_8(x) = x^7 + 2x^6 - 7x^5 - 12x^4 + 11x^3 + 10x^2 - 5x - 1$$
$$f_9(x) = x^7 + 2x^6 - 7x^5 - 13x^4 + 11x^3 + 14x^2 - 8x - 1$$
$$f_{10}(x) = x^7 + 2x^6 - 8x^5 - 18x^4 + 7x^3 + 23x^2 - x - 7$$
$$f_{11}(x) = x^7 + 3x^6 - 4x^5 - 11x^4 + 8x^3 + 7x^2 - 6x + 1$$
$$f_{12}(x) = x^7 + 3x^6 - 5x^5 - 17x^4 - 5x^3 + 9x^2 + 6x + 1.$$

Let x_i be a root of f_i $(i = 1, \ldots, 12)$. Then $x_5 = x_1^{-1}$ is immediate. To prove that all 12 fields are isomorphic is rather complicated. Extensive calculations by a computer show that they are indeed:

$$x_2 = x_1^6 + x_1^5 - 6x_1^4 - 5x_1^3 + 8x_1^2 + 4x_1 - 2$$
$$x_4 = x_1^2 - 2$$
$$x_5 = x_1^{-1}$$
$$x_7 = x_1^6 + x_1^5 - 6x_1^4 - 4x_1^3 + 8x_1^2 + x_1 - 2$$
$$x_8 = -x_1^5 - x_1^4 + 5x_1^3 + 4x_1^2 - 4x_1 - 2$$
$$x_9 = -x_1^6 + 6x_1^4 - x_1^3 - 8x_1^2 + 2x_1 + 2$$
$$x_{12} = -x_1^6 + 6x_1^4 - x_1^3 - 7x_1^2 + 2x_1$$
$$x_3 = x_7^5 - 5x_7^3 + 2x_7$$
$$x_{10} = -x_7^6 + 6x_7^4 - 7x_7^2 - x_7 + 1$$
$$x_{11} = x_7^5 + x_7^4 - 5x_7^3 - 5x_7^2 + 2x_7 + 2$$
$$x_6 = x_8^6 - 6x_8^4 + x_8^3 + 4x_8^2 - 3x_8 .$$

Theorem IV *There is—up to isomorphism—exactly one totally real algebraic number field F_0 of degree 7 and discriminant $d_{F_0} = d_0 \cdot F_0$ is generated by a root of the polynomial $x^7 + x^6 - 6x^5 - 5x^4 + 8x^3 + 5x^2 - 2x - 1$.*

Remark In the meantime I also proved that the galois group of F_0 is the symmetric group $\mathfrak{S}_7$ and that the class number of F_0 is 1. For the proofs and a system of fundamental units of F_0, see Pohst [5].

All computations were carried out on the IBM 370/165 of the Kernforschungsanlage Jülich.

REFERENCES

[1] J. Hunter, The minimum discriminant of quintic fields, *Proc. Glasgow Math. Assoc.* **3** (1957), 57–67.
[2] D. E. Knuth, "The Art of Computer Programming," Vol. 2, pp. 381–398. Addison-Wesley, Reading, Massachusetts, 1969.
[3] T. Nagell, Zur algebraischen Zahlentheorie, *Math. Z.* **34** (1931), 183–193.
[4] M. Pohst, Berechnung kleiner Diskriminanten total reeller algebraischer Zahlkörper, *J. Reine Angew. Math.* **278/279** (1975), 278–300.
[5] M. Pohst, Invarianten des total reellen Körpers siebten Grades mit Minimaldiskriminante, *Acta Arith.* **30** (1976), 199–207.
[6] H. Zassenhaus, On Hensel Factorization II, *Symposia Mathematica* **XV** (1975), 499–513.

AMS (MOS) 1970 subject classifications: 12A40, 12A45, 12A50.

On Absolutely Irreducible Representations of Orders †

WILHELM PLESKEN

TECHNISCHE HOCHSCHULE AACHEN
AACHEN, WEST GERMANY

Absolutely irreducible representation modules L of orders H over dedekind domains R with quotient field K are investigated. In particular a set of representatives of the R-classes contained in the K-class of L is described and the finiteness of the class number of L is investigated. The lattice of submodules of L is studied and the case where this lattice is distributive is characterized. This distributivity is necessary and sufficient for the class number of L to be finite in case the class number of R is finite and the residue class fields of R are infinite. The behavior of L under finite extensions of R and some examples of $\mathbb{Z}$-representations of finite groups are discussed.

1. Introduction

Let R be a dedekind domain with quotient field K and let H be an R-order. An H-representation module is defined as an H-module that is finitely generated and torsion free as an R-module. Two H-representation modules are R-equivalent if they are (H-) isomorphic, and they are K-equivalent if their tensor products with K are KH-isomorphic. (We write KH instead of $K \otimes_R H$.) Under certain conditions imposed on R the

† Supported by the Deutsche Forschungsgemeinschaft.

Jordan–Zassenhaus theorem [5, 16] assures that every K-equivalence class of H-representation modules splits into finitely many R-equivalence classes. In this paper we shall restrict our attention to absolutely irreducible H-representation modules. In Section 2 we describe a set of representatives of the R-classes lying in a given K-class of such a representation module (see Theorem 2.5). We show that a certain local–global principle is valid (see Proposition 2.6), which was already established by Maranda [10] in a slightly different way. Finally, we give two new proofs for the finiteness of the class number, one for general orders and one for group rings RG, where G is a finite group.

In Section 3 we investigate the lattice of submodules of an absolutely irreducible H-representation module L. In particular we characterize the case where this lattice is distributive (see Theorem 3.19) and discuss some restrictions on the lattice which can be derived from our proofs of the finiteness of the class number. Necessary and sufficient conditions are given for the class number of L to be finite.

In Section 4 we study the behavior of absolutely irreducible H-representation modules under finite extensions of the dedekind domain R.

In Section 5 finally some examples of absolutely irreducible $\mathbb{Z}$-representations of finite groups are discussed in order to give some applications and illustrations of the developed tools.

The author is greatly indebted to Professor H. Zassenhaus for many inspiring discussions and constant encouragement. He hereby wants to thank him.

2.

Let R be a dedekind domain with quotient field K and H an R-order. If two H-representation modules M and L are K-equivalent, then there exists a submodule N of L that is R-equivalent to M. For let $\varphi: KM \to KL$ be a KH-isomorphism. Because M is finitely generated as R-module there is an $r \in R$, $r \neq 0$ with $r\varphi(M) \subseteq L$. But $r\varphi: M \to r\varphi(M) \subseteq L$ via $x \to r\varphi(x)$ is certainly an H-isomorphism. So one can choose $N = r\varphi(M)$. N has the following properties:

(i) N is a H-submodule of L;
(ii) L/N is an (R-) torsionmodule; or equivalently
(ii') L and N have the same R-rank.

Definition 2.1 A submodule N of an H-representation module L with the properties (i) and (ii) is called a *centering* of L. The set of all centerings of L is denoted by $\mathfrak{Z}(L)$. (The term "centering" or "centered lattice" is used in crystallography.)

We have shown above that a set of representatives of the R-classes into which the K-class of L splits can be chosen as a subset of $\mathfrak{Z}(L)$. We ask, When are two centerings M and N of L R-equivalent? Let $\varphi: M \to N$ be an H-isomorphism. Then φ can be extended to an KH-isomorphism of KM onto KN, i.e., a KH-automorphism of KL, because $KM = KN = KL$. This proves the following lemma.

Lemma 2.2 *Two centerings M and N of L are R-equivalent if and only if there exists a KH-automorphism φ of KL with $\varphi(M) = N$.*

We assume now that L is absolutely irreducible. Then by Schur's lemma the KH-automorphisms of KL are just the multiplications with nonzero element of K. If R is a principal ideal domain, this remark and the invariant factor theorem suffice to prove the next proposition.

Proposition 2.3 *Let R be a principal ideal domain and L an absolutely irreducible H-representation module. A system of representatives of the R-classes lying in the K-class of L is given by the set $\mathfrak{R}(L)$ of all centerings of L that are not contained in rL for any nonunit r of R.*

Proof Compare Plesken [11] or Plesken and Pohst [12] for special cases. The proof follows from the more general Theorem 2.5. QED

If R is not a principal ideal domain, the most natural approach seems to be to work with ideals instead of numbers.

Definition 2.4 Let L be absolutely irreducible. $M, N \in \mathfrak{Z}(L)$ are called ideal equivalent if there is a (fractional) ideal $\mathfrak{A}$ of R with $M = \mathfrak{A}N$.

Hence R-equivalence implies ideal equivalence and ideal equivalence implies K-equivalence. It is immediately clear from the definition that the products $\mathfrak{A}M$ yield a system of representatives for the R-classes in $\mathfrak{Z}(L)$ where $\mathfrak{A}$ runs through a system of representatives of the ideal classes in R and M through a system of representatives of the ideal equivalence classes in $\mathfrak{Z}(L)$.

Theorem 2.5 *Let L be an absolutely irreducible H-representation module. A system $\mathfrak{R}(L)$ of representatives of the ideal equivalence classes in $\mathfrak{Z}(L)$ is given by all those centerings of L that are not contained in $\mathfrak{A}L$ for all integral ideals $\mathfrak{A}$ of R unequal to R. If $\mathfrak{I}$ is a set of representatives of the ideal classes of the ideals of R, a system of representatives of the R-equivalence classes of the RG-modules that are K-equivalent to L is given by $\{\mathfrak{A}M \mid \mathfrak{A} \in \mathfrak{I}$ and $M \in \mathfrak{R}(L)\}$.*

Proof Only the first part of the theorem is left to prove. Let M be a centering of L. By the invariant factor theorem for R-modules there exists element $m_1, \ldots, m_n$ in L, fractional ideals $\mathfrak{F}_1, \ldots, \mathfrak{F}_n$ of R, and integral ideals

$\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ of R with $\mathfrak{A}_1 \supseteq \mathfrak{A}_2 \supseteq \cdots \supseteq \mathfrak{A}_n$ such that

$$L = \mathfrak{F}_1 m_1 \oplus \mathfrak{F}_2 m_2 \oplus \cdots \oplus \mathfrak{F}_n m_n$$

and

$$M = \mathfrak{F}_1 \mathfrak{A}_1 m_1 \oplus \mathfrak{F}_2 \mathfrak{A}_2 m_2 \oplus \cdots \oplus \mathfrak{F}_n \mathfrak{A}_n m_n$$

(with the $\mathfrak{A}_i$ uniquely determined.) Then $\mathfrak{A}_1^{-1} M$ is in $\mathfrak{R}(L)$ showing that $\mathfrak{R}(L)$ contains at least one centering of each ideal equivalence class. Now let M and N be two ideal equivalent centerings of $\mathfrak{R}(L)$. Then $N = \mathfrak{B}M$ for some fractional ideal $\mathfrak{B}$ of R. By using the above decomposition of L and M once more, we get $\mathfrak{A}_1 = R$ and $\mathfrak{B}\mathfrak{A}_1 = R$ because M and N are in $\mathfrak{R}(L)$. Hence $\mathfrak{B} = R$ and $N = M$. QED

We can give a somewhat closer description of the set $\mathfrak{R}(L)$ if we use primary decomposition of the factor modules L/M with M in $\mathfrak{R}(L)$.

Proposition 2.6 *Every centering M in $\mathfrak{R}(L)$ is the intersection of uniquely determined centerings $M(\mathfrak{P})$ in $\mathfrak{R}(L)$ with $\mathfrak{P}$-power index in L, where $\mathfrak{P}$ is a prime dividing the index of M in L. Conversely, given finitely many elements $M(\mathfrak{P})$ in $\mathfrak{R}(L)$ with L: $M(\mathfrak{P})$ a $\mathfrak{P}$-power for different prime ideals $\mathfrak{P}$ of R, then the intersection of the $M(\mathfrak{P})$ is again in $\mathfrak{R}(L)$.*

Proof Let $M \in \mathfrak{R}(L)$. The $M(\mathfrak{P})$ are easily obtained from a primary decomposition of L/M. Let $L = \bigoplus_{i=1}^n \mathfrak{F}_i m_i$ and $M = \bigoplus_{i=1}^n \mathfrak{A}_i \mathfrak{F}_i m_i$ with $m_i \in L$, $\mathfrak{F}_i$ fractional ideals of R and $\mathfrak{A}_i$ integral ideals of R with $\mathfrak{A}_1 \supseteq \mathfrak{A}_2 \supseteq \cdots \supseteq \mathfrak{A}_n$. Let $\mathfrak{A}_n = \mathfrak{P}_1^{\alpha_1} \cdots \mathfrak{P}_k^{\alpha_k}$. Then $M(\mathfrak{P}_i) = \mathfrak{P}_i^{\alpha_i} L + M$ for $i = 1, \ldots, k$. Conversely, let $M(\mathfrak{P}_i)$ $(i = 1, \ldots, k)$ be centerings in $\mathfrak{R}(L)$ of $\mathfrak{P}_i$-power index, where the $\mathfrak{P}_i$ are different prime ideals. Let M be the intersection of the $M(\mathfrak{P}_i)$. M is in $\mathfrak{R}(L)$ iff the first invariant factor ideal of M in L is equal to R. But this factor ideal is the product of those of the $M(\mathfrak{P}_i)$, which are equal to R because the $M(\mathfrak{P}_i)$ are in $\mathfrak{R}(L)$. QED

Let $R_{\mathfrak{P}}$ denote the ring of $\mathfrak{P}$-regular elements in K. By standard results on localization of rings and modules one sees easily that for any centering M of L with $\mathfrak{B}$-power index we can view L/M as an $R_{\mathfrak{P}}$-module such that

$$L/M \underset{R_{\mathfrak{P}}H}{\cong} \mathfrak{A}L/\mathfrak{A}M \qquad \text{and} \qquad R_{\mathfrak{P}}M \underset{R_{\mathfrak{P}}H}{\cong} R_{\mathfrak{P}}\mathfrak{A}M$$

for any ideal $\mathfrak{A}$ of R. Using these remarks, Theorem 2.5, and Proposition 2.6, one easily derives Maranda's results [10] that (in our terminology) two centerings of L are ideal equivalent if and only if they are in the same genus, i.e., their localizations at all prime ideals of R are isomorphic, and that the class number of L is the product of the class numbers of R and those of $R_{\mathfrak{P}}L$ for all primes $\mathfrak{P}$ of R. It is also clear now that the determination of $\mathfrak{R}(L)$ can be reduced to that of the $\mathfrak{R}(R_{\mathfrak{P}}L)$ where $\mathfrak{P}$ runs through all primes such that

there is a centering between L and $\mathfrak{P}L$ or equivalently such that $L/\mathfrak{P}L$ becomes reducible as an H-module. Every centering M in $\mathfrak{R}(L)$ with $\mathfrak{P}$-power index in L is given by $R_{\mathfrak{P}}M \cap L$ with $R_{\mathfrak{P}}M$ in $\mathfrak{R}(R_{\mathfrak{P}}L)$. By Theorem 2.7 the other centerings of $\mathfrak{R}(L)$ are found by taking intersections. The problem to find $\mathfrak{R}(R_{\mathfrak{P}}L)$ remains.

Our next result implies that all elements of $\mathfrak{R}(L)$ lie between L and αL for a certain nonzero α in R. This implies the finiteness of $\mathfrak{R}(L)$ if the nontrivial factorings of R are finite. This is the Jordan–Zassenhaus theorem for the case that L is absolutely irreducible. If L is an H-representation module, then there is a homomorphism of H into $\mathrm{End}_R(L)$, $\phi_L\colon H \to \mathrm{End}_R(L)$ with $\phi_L(x)l = xl$ for all $x \in H$ and $l \in L$. Clearly $\phi_L(H)$ is a suborder of $\mathrm{End}_R(L)$, which leaves exactly the same submodules of L invariant as H. Furthermore, the R-module $\mathrm{End}_R(L)/\phi_L(H)$ is a torsion module.

Theorem 2.7 *Let L be absolutely irreducible and let $\mathfrak{A}$ be the last invariant factor ideal of $\phi_L(H)$ in $\mathrm{End}_R(L)$.*

(i) *If M is a centering of L with invariant factor ideals $\mathfrak{B}_1, \ldots, \mathfrak{B}_n$ in L, then $\mathfrak{B}_n\mathfrak{B}_1^{-1}$ divides $\mathfrak{A}$. In particular all centerings of $\mathfrak{R}(L)$ lie between L and $\mathfrak{A}L$.*

(ii) *If $\mathfrak{P}$ is a prime ideal dividing $\mathfrak{A}$, then either there is a centering in $\mathfrak{R}(L)$ with $\mathfrak{P}$-power index in L or $L/\mathfrak{P}L$ is irreducible but not absolutely irreducible as an $H/\mathfrak{P}H$-module. (By tensoring with a suitable extension ring this last situation can be reduced to the first.) (The prime divisors of $\mathfrak{A}$ are sometimes called critical primes.)*

Proof (i) By the invariant factor theorem there are elements $m_i \in L$, fractional ideals $\mathfrak{F}_i$ of R and integral ideals $\mathfrak{A}_i$ of R for $i = 1, \ldots, n$ such that $L = \bigoplus_{i=1}^n \mathfrak{F}_i m_i$, $M = \bigoplus_{i=1}^n \mathfrak{A}_i\mathfrak{F}_i m_i$ and $\mathfrak{A}_i \mid \mathfrak{A}_{i+1}$ for $i = 1, \ldots, n-1$. Hence we can identify $\mathrm{End}_R(L)$ with the ring of matrices $\{(a_{kl}) \mid a_{kl} \in \mathfrak{F}_k^{-1}\mathfrak{F}_l$ $(k, l = 1, \ldots, n)\}$. By identifying $\mathrm{End}_R(M)$ with the corresponding ring of matrices one sees that the last invariant factor of $\mathrm{End}_R(L) \cap \mathrm{End}_R(M)$ in $\mathrm{End}_R(L)$ is $\mathfrak{B}_1^{-1}\mathfrak{B}_n$. Because $\phi_L(H)$ is contained in $\mathrm{End}_R(L) \cap \mathrm{End}_R(M)$, we get $\mathfrak{B}_1^{-1}\mathfrak{B}_n \mid \mathfrak{A}$.

(ii) Let $\mathfrak{P} \mid \mathfrak{A}$. Then those endomorphisms of $L/\mathfrak{P}L$ induced by H cannot be the full $R/\mathfrak{P}$-endomorphism ring of $L/\mathfrak{P}L$ which is isomorphic to $(R/\mathfrak{P})^{n\times n}$. If there are proper H-submodules of $L/\mathfrak{P}L$, the first assertion holds. If not, $L/\mathfrak{P}L$ is irreducible and the image of H in $\mathrm{End}_{R/\mathfrak{P}}(L/\mathfrak{P}L)$ is isomorphic to $D^{k\times k}$ where D is a skew field containing $R/\mathfrak{P}$ properly by the remark above. QED

We remark that the last invariant factor of $\phi_L(H)$ in $\mathrm{End}_R(L)$ depends on the R-class of L. If H is the group ring RG of a finite group G such that the characteristic of R does not divide $|G|$, then we can prove by using Schur's

relations [5, 8], that all centerings in $\mathfrak{R}(L)$ lie between L and $(|G|/n)L$, where n is the R-rank of L. In Brauer [2] and Brauer and Nesbitt [3], Schur's relations have been used in a similar way.

Theorem 2.8 *Let G be a finite group and L an absolutely irreducible RG-representation module, where the characteristic of R does not divide $|G|$. If M is a centering of L with invariant factor ideals $\mathfrak{B}_1, \ldots, \mathfrak{B}_n$ (n = R-rank of L), then $|G|/n$ lies in $\mathfrak{B}_n \mathfrak{B}_1^{-1}$. In particular all centerings in $\mathfrak{R}(N)$ lie between N and $(|G|/n)N$ for any $N \in \mathfrak{Z}(L)$.*

Proof As in the proof of Theorem 2.7 let $L = \bigoplus_{i=1}^{n} \mathfrak{F}_i m_i$ and $M = \bigoplus_{i=1}^{n} \mathfrak{B}_i \mathfrak{F}_i m_i$. Let D be the K-representation of G belonging to KL with respect to the basis $m_1, \ldots, m_n$. If $D(g) = (d_{ij}(g))$ for $g \in G$, then Schur's relations assure that

$$\delta_{il}\delta_{jk}\frac{|G|}{n} = \sum_{g \in G} d_{ij}(g) d_{kl}(g^{-1}).$$

The invariance of the lattices L and M respectively implies $d_{st}(h) \in \mathfrak{F}_s \mathfrak{F}_t^{-1}$ and $d_{st}(h) \in \mathfrak{B}_s \mathfrak{F}_s \mathfrak{B}_t^{-1} \mathfrak{F}_t^{-1}$ for all $h \in G$ and $1 \leq s, t \leq n$. By taking $h = g$, $s = i$, $t = j$, and $h = g^{-1}$, $s = j$, $t = i$ we get

$$|G|/n \in \mathfrak{F}_j \mathfrak{F}_i^{-1} \mathfrak{B}_j^{-1} \mathfrak{F}_j^{-1} \mathfrak{B}_i \mathfrak{F}_i = \mathfrak{B}_i \mathfrak{B}_j^{-1}.$$

This implies the theorem if we choose $i = n$ and $j = 1$. QED

Corollary 2.9 *If under the assumption of Theorem 2.8 $|G|/n$ is a unit in R, then $\mathfrak{R}(L)$ consist only of L.*

Corollary 2.10 *Under the assumption of Theorem 2.8 the K-class of L splits into finitely many R-classes if and only if the ideal class group of R is finite.*

It is clear that Theorem 2.8 imposes stronger restrictions on RG-representation modules concerning the finiteness of the class number than Theorem 2.7 does for H-representation modules. For instance, Theorem 2.8 implies that the class number of an irreducible $\mathbb{C}[x]G$-representation module is 1, whereas there are certainly $\mathbb{C}[x]$ orders H with modules having an infinite class number. For instance,

$$H = \left\langle \mathbb{C}[x]\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, x\mathbb{C}[x]^{2\times 2} \right\rangle$$

has $L = \mathbb{C}[x]^{2\times 1}$ as a representation module in the obvious way. The class number is infinite; in fact those centerings of $\mathfrak{R}(L)$ that lie properly between L and xL are in one-to-one correspondence with the points of the complex projective line. In Corollary 3.9 we shall be able to give necessary and

sufficient conditions for an absolutely irreducible H-representation module to have a finite $\mathfrak{R}(L)$.

3.

In this section we want to investigate the lattice $\mathfrak{Z}(L)$ of centerings of L. Throughout the whole section we assume R to be a principal ideal domain if not otherwise stated. (This is legitimate because of the results of the preceding section.) We shall first prove a somewhat stronger version of Brauer and Nesbitt's result that the composition factors of M/pM for $M \in \mathfrak{Z}(L)$ are the same as of L/pL where p is a prime element of R. We need not assume irreducibility for this.

Definition 3.1 Let M, M', N, N' be centerings of L with $M' \subset M$ and $N' \subset N$.

(i) The pair (M, M') is projectively neighbored to (N, N'), if either

(a) $M \subset N$ and $M' = M \cap N'$ (Fig. 1) or
(b) $N \subset M$ and $N' = N \cap M'$.

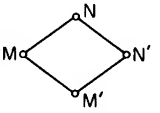


FIG. 1

(ii) (M, M') and (N, N') are projectively related if there is a chain of pairs of centerings (L_1, L_1'), (L_2, L_2'), ..., (L_k, L_k') with $(L_1, L_1') = (M, M')$, $(L_k, L_k') = (N, N')$ such that (L_i, L_i') is either projectively neighbored to (L_{i+1}, L_{i+1}') or there is an $\alpha \in K$ with $(L_{i+1}, L_{i+1}') = (\alpha L_i, \alpha L_i')$.

It is clear that "being projectively related" is an equivalence relation on the pairs (M, M') of centerings of L with $M' \subset M$. If (M, M') and (N, N') are projectively related, then M/M' and N/N' are isomorphic. The converse is not always true. The first fundamental result is the following theorem generalizing the Jordan–Hölder theorem for our situation.

Theorem 3.2 *Let L be a (not necessarily irreducible) H-representation module with R a principal ideal domain, let p be a prime element in R, and let M be a centering of L. For any two H-composition series*

$$L_1 = L > L_2 > \cdots > L_k = pL \qquad \text{and} \qquad M_1 = M > M_2 > \cdots > M_l = pM$$

of L/pL and M/pM respectively, $l = k$ holds and there exists a permutation π of

the k indices such that (L_i, L_{i+1}) *is projectively related to* $(M_{\pi(i)}, M_{\pi(i)+1})$ *for* $i = 1, \ldots, k-1$.

Proof Any two composition series of N/pN are projectively related in the above sense for any centering N of L, which is easily seen from the Schreier–Zassenhaus proof of the Jordan–Hölder theorem. (Note R/pR is a field.) It suffices to prove the theorem under the assumption that L/M is a simple RG-module. If $M \not\supseteq pL$, the result is trivial. If $M \supset pL$, we choose $L_2 = M$ and $M_{l-1} = pL$. Then one sees immediately that (L, M) is projectively related to (pL, pM) and (M, pL) to itself (Fig. 2). The theorem follows. QED

FIG. 2

As a corollary we get the well-known result first proved by Brauer and Nesbitt under the assumption that H is a group ring [4].

Corollary 3.3 *Under the assumption of Theorem* 3.2 *the irreducible constituents of* $R/pR \otimes_R H$*-representations belonging to* L/pL *and* M/pM *are the same.*

This corollary is the basis for the following algorithm developed by Plesken [11] to compute $\mathfrak{R}(L)$ for absolutely irreducible L (if $\mathfrak{R}(L)$ is finite). Assuming that $A_1, \ldots, A_k$ are the irreducible constituent of L/pL for all primes p for which L/pL becomes reducible. (These are only finitely many primes by Theorem 2.7.) From any $M \in \mathfrak{Z}(L)$ new centerings are obtained as the kernels of all possible epimorphism of M onto the A_i. Determining these epimorphisms as well as their kernels amounts to solving systems of linear equations over the field R/pR with p as above. Starting out with this procedure from L one has to test for each new centering N whether it lies in $\mathfrak{R}(L)$ (and does not have to compare it with all the previous ones one has obtained), i.e., one has to check whether the first invariant factor of N in L is a unit. This procedure eventually yields all centerings of $\mathfrak{R}(L)$ (if $\mathfrak{R}(L)$ is finite). For details, the reader is referred to Plesken [11] or Plesken and Pohst [12].

Before we proceed investigating the lattice $\mathfrak{Z}(L)$ we make two simple remarks.

(1) From the idea of the algorithm it is clear that $\mathfrak{R}(L)$ consists of L

alone iff for all primes p of R the module L/pL stays irreducible. Let R have the property that for all prime ideals of R the factor field has the same characteristic as R. If $H = RG$ for a finite group G, then $|\mathfrak{R}(L)| = 1$ independent of the characteristic of R. More generally, if an order H' over any dedekind domain $R' \supseteq R$ with an absolutely irreducible representation module L' contains an R-order H with an absolutely irreducible representation module L such that $H' = R' \otimes_R H$ and $L' = R' \otimes_R L$, then $\mathfrak{R}(L')$ consists only of L' in case R is a field.

(2) The second remark refers to the ideas developed by Schur in [13]. We assume R is a dedekind domain. One can predict the Steinitz invariants of the centerings of L if one knows the Steinitz invariant of L and the indices of all centerings in $\mathfrak{R}(R_{\mathfrak{P}} L)$ for all those critical primes $\mathfrak{P}$ which are not in an ideal class of the nth power of some other ideal ($n = R$-rank of L). If for instance the exponent of the ideal class group of R divides the $R/\mathfrak{P}$-rank of all irreducible constituents of $L/\mathfrak{P}L$ for all critical primes $\mathfrak{P}$, then all centerings of L have the same Steinitz invariant. It would be interesting to find a Dedekind ring R, a finite group G, and an RG-representation module L such that the Steinitz invariants of all centerings of L are not principal, i.e., the matrix representation of KL cannot be transformed into one where all matrix entries lie in R.

We come back to the lattice $\mathfrak{Z}(L)$ and assume L to be absolutely irreducible of R-rank n and R to be a principal ideal domain. The lattice is modular and by Proposition 2.6 splits into the direct product of the sublattices $\mathfrak{Z}_p(L)$ of the p-centerings, as we want to call the centerings with p-power index in L (p a prime of R). For noncritical primes p, the p-centerings of L are given by $p^\alpha L$ with $\alpha \in \mathbb{Z}^{\geq 0}$. Further $\mathfrak{Z}(L)$ is periodic in the sense that $\mathfrak{Z}(L)$ is the disjoint union of all $\mathfrak{A}\mathfrak{R}(L)$ with $\mathfrak{A}$ running through all integral ideals of R. We first want to discuss restrictions imposed on $\mathfrak{Z}(L)$ by Theorems 2.7 and 2.8.

Definition 3.4 The biggest $\alpha \in \mathbb{Z}^{\geq 0}$ such that p^α is the last invariant factor of M in N with $M, N \in \mathfrak{Z}_p(L)$ and $M \in \mathfrak{R}(N)$ is called the critical p-exponent of L for any prime p of R.

We note that Theorem 2.8 yields an upper bound for the critical p-exponent in the case $H = RG$, namely the biggest α with $p^\alpha | (|G|/n)$. Theorem 2.7, however, does not give such a bound immediately. But using Theorem 2.7 and the kind of argument used in its proof, one gets 2α as an upper bound for the critical p-exponent, where p^α divides the last invariant factor of $\phi_L(H)$ in $\mathrm{End}_R(L)$ but not $p^{\alpha+1}$ (compare Theorem 2.7 for the terminology). Hence the critical p-exponent is always well defined.

Theorem 3.5 *Let $M, N \in \mathfrak{Z}_p(L)$ for some prime p of R such that $M, N \neq$*

$M + N$. Then $M, N \in \mathfrak{R}(M + N)$. If p^α and p^β are the last invariant factor of M, resp. N, in $M + N$, then $\alpha + \beta$ is smaller than or equal to the critical p-exponent of L.

Proof The first statement follows easily if one chooses compatible bases for N and M and uses these bases to construct a basis for $N + M$ in an obvious way. From the second isomorphism theorem we conclude that α is the smallest natural number such that $p^\alpha N \subseteq M$, hence $p^\alpha N \in \mathfrak{R}(M)$ (Fig. 3).

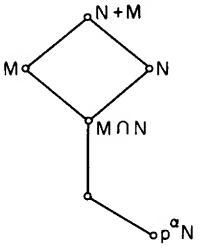


FIG. 3

Clearly $p^{\alpha+\beta}(M/p^\alpha N) = 0$. If $p^\gamma M \subseteq p^\alpha N$ with $\gamma < \alpha + \beta$, this would contradict the definition of β as the p-exponent of the last invariant factor of

$$N + M/N \cong M/M \cap N \cong (M/p^{\gamma-\alpha}M)/(M \cap N/p^{\alpha-\gamma}M). \quad \text{QED}$$

As a first corollary we get a result first proved by Brauer in [2].

Corollary 3.6 *Let H be a group ring RG and p be a prime of R. If $p \mid (\mid G \mid /n)$ but $p^2 \nmid (\mid G \mid /n)$, then the p-centerings are linearly ordered and $\mathfrak{R}(L) \cap \mathfrak{Z}_p(L)$ consists of those $M \in \mathfrak{Z}(L)$ with $pL \not\leq M \leq L$.*

We want to ask now, How many maximal centerings N_i of $N \in \mathfrak{Z}(L)$ can exist such that the N/N_i are all isomorphic to each other?

Lemma 3.7 *Let $N \in \mathfrak{Z}(L)$ and let A be an irreducible constituent of L/pL. Then $\mathrm{Hom}_H(N, A)$ is a vector space over $\mathrm{End}_H(A)$, the dimension of which is bounded by the multiplicity of A in L/pL. The centerings M of N with $N/M \cong \bigoplus_{i=1}^k A$ are in one-to-one correspondence with the k-dimensional subspaces of $\mathrm{Hom}_H(N, A)$ (over $\mathrm{End}_H(A)$).*

Proof For $\varphi \in \mathrm{Hom}_H(N, A)$ and $\alpha \in \mathrm{End}_R(A)$, we get

$$\alpha \circ \varphi \in \mathrm{Hom}_H(N, A).$$

Since A is irreducible, $\mathrm{End}_R(A)$ is a skew field. So $\mathrm{Hom}_H(N, A)$ is a $\mathrm{End}_R(A)$-vector space. Now the rest of the statements follows easily. QED

Corollary 3.8 *If under the assumption of Lemma 3.7 the field R/pR is*

finite of q elements, then the number of the $M \in \mathfrak{Z}(N)$ *with* $N/M \cong A$ *is of the form* $(q^{\alpha\beta} - 1)/(q^{\alpha} - 1)$ *with* $\alpha = \dim_{R/pR} \mathrm{End}_H(A)$ *and* $\beta \leq$ *multiplicity of A in* L/pL.

Corollary 3.9 *Let the fields* R/pR *be infinite for the critical primes p of R. Then* $\mathfrak{R}(L)$ *is finite if and only if for any two* $N, M \in \mathfrak{Z}(L)$ *with* $N \subset M$ *and N maximal in M there is no other centering* N' *of M with* $M/N \cong M/N'$.

Proof Follows immediately from Lemma 3.7 and Theorem 2.7. QED

As an important consequence we remark that there is at most one centering M of N with $N/M \cong A$ in case the multiplicity of A in L/pL is one. We want to prove that there always exist a centering N of L that does not only have the property that there is only one centering $M \subset N$ with $N/M \cong A$ but also has M as the only maximal p-centering. We can even do better than this by introducing a new type of constituent of L/pL using the ideas of Definition 3.1 and Theorem 3.2.

Definition 3.10 Let N be a centering of L and let $N_1 = N > N_2 > \cdots > N_k = pN$ be a composition series of N/pN. We call the projective equivalence classes of the pairs (N_i, N_{i+1}) the projective composition factors of N/pN $(i = 1, \ldots, k-1)$. The multiplicity of such a composition factor is the number of the indexes i $(i = 1, \ldots, k-1)$ with (N_i, N_{i+1}) lying in this equivalence class.

It is clear from Theorem 3.2 that the definition of projective composition factor does not depend on the chosen centering N. If (N, M) belongs to a projective composition factor of L/pL, then N/M is (an ordinary) composition factor of L/pL. However, (N_1, M_1) and (N_2, M_2) may belong to different projective composition factors of L/pL though N_1/M_1 is isomorphic to N_2/M_2. So in general there are more projective composition factors than ordinary ones and the multiplicities of the projective ones are smaller. It is clear that both concepts are the same if L/pL does not have repeated (ordinary) composition factors.

Theorem 3.11 *Let* (M, M') *belong to a projective composition factor of* L/pL. *Then there is a p-centering N of L such that N has exactly one maximal p-centering* N'. *Further,* (N, N') *is projectively equivalent to* (M, M').

Proof Let N be a p-centering of M with the following properties: (i) $N \not\subseteq M'$; (ii) there is no p-centering $\tilde{N}$ of M contained in N with property (i). By Theorem 3.5 each N with (i) is contained in $\mathfrak{R}(M)$. By Theorem 2.7 there exists an N with (i) and (ii) (though it might not be unique). N satisfies the assertion of the theorem (possibly after multiplication with an element of K to make it a p-centering). Take $N' = M' \cap N$. If there were a maximal p-centering N'' of N with $N'' \neq N$, then N'' is a p-centering of M satisfying

(i); hence N does not satisfy (ii), which is a contradiction. QED

We now want to investigate those lattices of centerings that have the property that for any projective composition factor and any centering M there is at most one centering M' of M such that (M, M') belongs to the given composition factor.

Proposition 3.12 *The lattice of centerings of L is distributive if and only if it satisfies the following condition:*

(*) *For any projective composition factor C of L and any centering M of L there exists at most one centering M' of M with (M, M') belonging to C.*

Proof This is an immediate corollary of Birkhoff's theorem [1] that a modular lattice is distributive if and only if it does not contain sublattices of the form shown in Fig. 4. Another proof follows from Lemma 3.16. QED

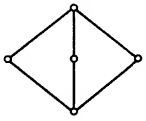


FIG. 4

Proposition 3.13 *Let L satisfy condition (*) of Proposition 3.12. If $M, N, N' \in \mathfrak{Z}(L)$ with $N, N' \subseteq M$ such that M/N and M/N' have the same projective composition factors (with the same multiplicities), then $N = N'$.*

Proof We use induction on the number of composition factors of M/N. If this number is one, the theorem follows from (*) immediately. Assume the theorem is true if M/N has less than m composition factors (multiplicities counted!). If there is a centering M' of M, unequal to M and containing both N and N' we can apply the induction hypothesis. Let

$$M = N_0 > N_1 > \cdots > N_m = N$$

$$M = N'_0 > N'_1 > \cdots > N'_m = N'$$

be composition series of M/N and M/N'. Let i be the smallest index such that (N'_i, N'_{i+1}) belongs to the same projective composition factor as (N_0, N_1). Then the composition series of M/N' can be replaced by $M = N''_0 > N''_1 > N''_2 > \cdots > N''_m = N'$ where $N''_j = N'_{j-1} \cap N_1$ for $j = 1, 2, \ldots, i$ and $N''_j = N'_j$ for $j = i+1, \ldots, m$. Note that $N'_{i+1} = N'_i \cap N_1$. Because of $N_1 = N''_1$ the induction hypothesis can be applied. QED

Proposition 3.14 *Under assumption (*) of Proposition 3.12 the projective composition factors of L/pL have multiplicity one.*

Proof Let $L = L_1 > L_2 > \cdots > L_k = pL$ be a composition series of

L/pL. Let (L_i, L_{i+1}) be projectively equivalent to (L_j, L_{j+1}) with $i < j$. Then there is a chain $(N_1, N_1'), (N_2, N_2'), \ldots, (N_s, N_s')$ of pairs of centerings such that $(N_1, N_1') = (L_i, L_{i+1})$ and $(N_s, N_s') = (p^\alpha L_j, p^\alpha L_{j+1})$ for some $\alpha \in \mathbb{N}$ and (N_k, N_k') is a projective neighbor of (N_{k+1}, N_{k+1}'). But $(*)$ implies that (N_k, N_{k+1}) or (N_{k+1}, N_k) (respectively if $N_k \geq N_{k+1}$ or if $N_{k+1} \geq N_k$) is not projectively equivalent to (L_i, L_{i+1}). Hence if M is a centering containing all the N_k, the multiplicity of (L_i, L_{i+1}) in M/N_i is the same for all N_i. So (L_i, L_{i+1}) cannot be projectively equivalent to (L_j, L_{j+1}). QED

Definition 3.15 Assume $(*)$ of Proposition 3.12 and let $L = L_1 > L_2 > \cdots > L_{k+1} = pL$ be a fixed composition series of L/pL. Let M, N be p-centerings of L with $M \subseteq N$. We denote M by $N(\alpha_1, \ldots, \alpha_k)$ where α_i $(i = 1, \ldots, k)$ are the multiplicities of the projective composition factor (L_i, L_{i+1}) in N/M.

Lemma 3.16 *Under the assumption* $(*)$ *of Proposition* 3.12 *and in the terminology of Definition* 3.15 *the following hold:*

(i) $p^\alpha N(\alpha_1, \ldots, \alpha_k) = N(\alpha + \alpha_1, \ldots, \alpha + \alpha_k)$ *for* $\alpha \in \mathbb{Z}^{\geq 0}$;

(ii) $N(\alpha_1, \ldots, \alpha_k) \cap N(\beta_1, \ldots, \beta_k) = N(\gamma_1, \ldots, \gamma_k)$ *with* $\gamma_i = \max(\alpha_i, \beta_i)$ $(i = 1, \ldots, k)$;

(iii) $N(\alpha_1, \ldots, \alpha_k) + N(\beta_1, \ldots, \beta_k) = N(\delta_1, \ldots, \delta_k)$ *with* $\delta_i = \min(\alpha_i, \beta_i)$ $(i = 1, \ldots, k)$;

(iv) $N(\alpha_1, \ldots, \alpha_k)(x_1, \ldots, x_k) = N(\alpha_1 + x_1, \ldots, \alpha_k + x_k)$;

(v) $N(\alpha_1, \ldots, \alpha_k) \in \mathfrak{R}(N)$ *iff at least one* $\alpha_i = 0$; *where* $N(\alpha_1, \ldots, \alpha_k)$, $N(\beta_1, \ldots, \beta_k)$, *and* $N(\alpha_1, \ldots, \alpha_k)(x_1, \ldots, x_k)$ *are p-centerings of* N.

Proof (i) and (iv) are trivial. We prove (ii) and (iii), i.e., $\gamma_i = \max(\alpha_i, \beta_i)$ and $\delta_i = \min(\alpha_i, \beta_i)$. From the second isomorphism theorem we see immediately that the first set of equations implies the second. To proof the first equations one proceeds similarly to the proof of Proposition 3.13 by using induction on $\sum_{i=1}^k \alpha_i + \sum_{i=1}^k \beta_i$. QED

Our next aim is to describe the biggest R-order in $\mathrm{End}_K(KL)$ that leaves all the centerings of L invariant. Of course it is given by $\bigcap_{M \in \mathfrak{R}(L)} \mathrm{End}_R(M)$ where we view the $\mathrm{End}_R(M)$ as orders of $\mathrm{End}_K(KL)$. We shall prove that this is a graduated order as introduced by Zassenhaus [14] iff $\mathfrak{Z}(L)$ satisfies $(*)$ of Proposition 3.12.

Definition 3.17 Let R be a local Dedekind ring with prime element p. A graduated order over R is a suborder of $R^{n \times n}$ containing n orthogonal primitive idempotents $e_1, \ldots, e_n$ with $e_1 + \cdots + e_n = I_n$ (= unit matrix).

We give a short summary of the properties of graduated orders [14].

Theorem 3.18 *Let* A *be a graduated order contained in* $R^{n \times n}$ *with primitive idempotents* $e_1, \ldots, e_n$ (*and* R *local*). A *can be transformed in such a way*

that the e_i become the diagonal matrices $\operatorname{diag}(0, \ldots, 0, 1, 0, \ldots, 0)$ *with the* 1 *in the* ith *place; and further there are natural numbers* $n_1, \ldots, n_k$ *with* $n_1 + \cdots + n_k = n$ *and* $\alpha_{ij} \in \mathbb{Z}^{\geq 0} \cup \{\infty\}$ $(i = 1, \ldots, k)$ *such that* $\alpha_{ij} = \infty$ *only if* $i \neq j$ *and* $\alpha_{ii} = 0$ *and*

$$A = \{(p^{\alpha_{ij}} a_{ij}) \mid a_{ij} \in R^{n_i \times n_j}\}$$

where p^∞ *stands for zero. The* α_{ij} *satisfy the obvious conditions*

$$\alpha_{ij} + \alpha_{jl} \geq \alpha_{il} \qquad (i, j, k = 1, \ldots, l)$$

which are necessary and sufficient for A to be closed under multiplication. $KA = K^{n \times n}$ *iff all* $\alpha_{ij} \in \mathbb{Z}^{\geq 0}$. *In this case the submodules (centerings) of* $R^{n \times 1}$ *invariant under left multiplication are given by*

$$R^{n \times 1}(\alpha_1, \ldots, \alpha_k) = \left\{ \begin{pmatrix} p^{\alpha_1} a_1 \\ \vdots \\ p^{\alpha_k} a_k \end{pmatrix} \text{ with } \alpha_{ij} d_j \geq \alpha_i \quad a_j \in R^{n_j \times 1} \text{ for } j = 1, \ldots, k \right\}.$$

If R is a nonlocal principal ideal domain, then a suborder of $R^{n \times n}$ is called a graduated order if it becomes a graduated order by localization at all primes p of R. Theorem 3.18 can be generalized in an obvious way for this situation. From Theorem 3.18 we see that the centerings of an irreducible graduated order form a distributive lattice because the rules of Lemma 3.16 are fulfilled. We also have compatible bases for the centerings of $R^{n \times 1}$ in the sense of Zassenhaus [17], i.e., one gets a basis of each centering by multiplying the elements of the basis,

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix},$$

by certain elements of R. We can now characterize the modules satisfying $(*)$ in Proposition 3.12.

Theorem 3.19 *Let L be an absolutely irreducible representation module of an R-order H where R is a principal ideal domain. The following statements are equivalent:*

(i) *L satisfies condition* $(*)$ *in Proposition* 3.12.

(ii) *The lattice* $\mathfrak{Z}(L)$ *of centerings of L is distributive.*

(iii) *For all prime elements p of R the multiplicity of the projective composition factors of L/pL is equal to one.*

(iv) *There exists a system of compatible bases for the centerings of L.*

(v) *The maximal suborder of* $\operatorname{End}_R(L)$ *leaving all the centerings of L invariant is a graduated R-order of* $K^{n \times n}$.

Proof In Proposition 3.12 we proved already that (i) and (ii) are equivalent. By Proposition 3.14 statement (i) implies (iii); the converse of this is trivial. By Theorem 3.18 the last two statements are equivalent and also by Theorem 3.18 one sees that (v) implies (i). We show that (i) implies (iv). In Zassenhaus [17] necessary and sufficient conditions for the existence of compatible bases for systems of submodules of a finitely generated abelian group are given. The results of Zassenhaus [17] can easily be generalized to finitely generated modules over principal ideal domains in an obvious way. To prove (iv) we then have to check the following conditions for $\mathfrak{Z}(L) = \Sigma$:

(a) $\mathfrak{Z}(L)$ is distributive.

(b) For any prime p of R, let Σ_p be the set of all factor modules $M/p^\alpha L$, where α is the critical p-exponent of L and $M \in \mathfrak{Z}(L)$ with $p^\alpha L \subseteq M$.

(b_1) $p^\mu(m_1 \cap m_2) = p^\mu m_1 \cap p^\mu m_2$ for all $\mu \in \mathbb{Z}^{\geq 0}$ and $m_1, m_2 \in \Sigma_p$.

(b_2) Let $m \in \Sigma$, $m' = \sum_{m'' \in \Sigma} (p^\nu m'') \cap m$ and define $(p^{-\nu}, \Sigma)m$ to be the intersection of all $m'' \in \Sigma$ with $p^\nu m'' = m'$. For any $\nu \in \mathbb{Z}^{\geq 0}$ the operator $(p^{-\nu}, \Sigma)$ has to satisfy the $(p^{-1}, \Sigma)(p^{-\nu}, \Sigma)m = (p^{-(\nu+1)}, \Sigma)m$ for all $m \in \Sigma$.

Condition (a) is satisfied because of Proposition 3.12. One easily checks (b_1) by means of Lemma 3.16. We check (b_2). Let $m = L(\alpha_1, \ldots, \alpha_k)/p^\alpha L \in \Sigma$. If $\nu \geq \alpha$ we get $(p^{-\nu}, \Sigma)m = p^\alpha L/p^\alpha L$. If $\nu < \alpha$, one sees easily $(p^{-\nu}, \Sigma)m = L(\beta_1, \ldots, \beta_k)/p^\alpha I$ with $\beta_i = \max(\nu, \alpha_i) - \nu$. ($b_2$) now follows easily. QED

The following application of Theorem 3.19 which is already partly proved in Zassenhaus [17] might be of interest.

Corollary 3.20 *Let R be a principal ideal domain, L a finitely generated free R-module, and let $\mathfrak{M}$ be a finite set of submodules of L of the same R-rank as L. Then there exist compatible bases for L and the submodules in $\mathfrak{M}$ if and only if the lattice $\mathfrak{M}$ is distributive, where $\mathfrak{M}$ is generated by L and the elements of $\mathfrak{M}$ by taking intersections, sums, and by multiplying with elements of the quotient field of R such that the resulting modules are contained in L.*

Proof Let $H = \mathrm{End}_R(L) \cap \bigcap_{M \in \mathfrak{M}} \mathrm{End}_R(M)$, where $\mathrm{End}_R(M)$ is considered to be an order in $\mathrm{End}_K(KM)$. Then H is an R-order and L an absolutely irreducible H-representation module with $\mathfrak{M} \subseteq \mathfrak{Z}(L)$. That the existence of compatible bases implies the distributivity of $\mathfrak{M}$ was already observed in [17]. (This can also be obtained by applying Theorem 3.19.) As for the converse we apply a slight generalization of Theorem 3.19. One sees easily that the distributivity of $\mathfrak{M}$ implies condition (*) of Proposition 3.12 for $\mathfrak{M}$. From this one concludes that the results in Propositions 3.13 and 3.14 and Lemma 3.16 are also valid for $\mathfrak{M}$, as well as the version of Theorem 3.19 for $\mathfrak{M}$ instead of $\mathfrak{Z}(L)$. If at some place the finiteness of the critical p-exponents is used, the arguments are still valid, since these exponents are also finite for $\bar{\mathfrak{M}}$ because of $\bar{\mathfrak{M}} \subseteq \mathfrak{Z}(L)$. Now this version of Theorem 3.19

shows that there is a system of compatible bases even for all modules in $\mathfrak{M}$. This finishes the proof. We remark, however, that one can conclude now by using Theorem 3.18 that $\mathfrak{Z}(L)$ and $\bar{\mathfrak{M}}$ are equal. QED

The next corollary of the proof of Corollary 3.20 can be considered as a partial converse of Theorem 2.7.

Corollary 3.21 *Let R be a principal ideal domain on L, a finitely generated free R-module. Let $\mathfrak{M}$ be a finitely generated (in the sense of Corollary 3.20) lattice of submodules of L that have the same R-rank as L. Then the maximal suborder H of $\mathrm{End}_R(L)$ leaving the modules in $\mathfrak{M}$ invariant has the same R-rank as $\mathrm{End}_R(L)$ and L is an absolutely irreducible H-representation module. (It might happen that $\mathfrak{M} \subset \mathfrak{Z}(L)$.)*

The next application of the ideas developed in this chapter can already be found in Plesken [11].

Theorem 3.22 *If L/pL has two projective constituents each with multiplicity one, then there is a centering M of L such that the p-centerings in $\mathfrak{R}(M)$ are linearly ordered. M can be chosen to be any centering of L such that M/pM is indecomposable.*

Proof The proof follows from Theorem 3.11 and Lemma 3.16. In the notation of Definition 3.15:

$$\mathfrak{Z}_p(L) \cap \mathfrak{R}(M) = \{M(0, 0), M(1, 0), \ldots, M(\delta, 0)\}$$

$$\text{or} \qquad \{M(0, 1), \ldots, M(0, \delta)\}. \quad \text{QED}$$

We finish this section with a complete list of distributive lattices of p-centerings of L, where L/pL has three composition factors, and the critical p-exponent α of L is less than or equal to three. So we have the combinatorial task of finding all graduated orders as described in Theorem 3.18 with $l = 3$ and $\alpha_{ij} + \alpha_{ji} \leq 3$. Note that $\max_{i,j}(\alpha_{ij} + \alpha_{ji})$ is the critical p-exponent of L. If the critical p-exponent α is one, the centerings are linearly ordered. If $\alpha = 2$, there are four possibilities and for $\alpha = 3$ seven possibilities: The maximal H order leaving the centerings invariant can be transformed to

$$H(\alpha_{21}, \alpha_{23}, \alpha_{31}, \alpha_{32}) = \left\{ \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ p^{\alpha_{21}} a_{21} & a_{22} & p^{\alpha_{23}} a_{23} \\ p^{\alpha_{31}} a_{31} & p^{\alpha_{32}} a_{32} & a_{33} \end{bmatrix} \;\middle|\; a_{ij} \in R^{n_i \times n_j} \right\}$$

with $(\alpha_{21}, \alpha_{23}, \alpha_{31}, \alpha_{32})$ equal to (1, 0, 2, 1), (1, 0, 2, 2), (2, 0, 2, 2), and (2, 1, 2, 1) for $\alpha = 2$, and (1, 0, 3, 2), (1, 0, 3, 3), (2, 0, 3, 2), (2, 0, 3, 3), (2, 1, 3, 2),

(3, 1, 3, 2), and (3, 0, 3, 3) for $\alpha = 3$. The class numbers are 4, 5, 6, 7, 6, 7, 8, 9, 8, 11, 10. The lattices are shown in Fig. 5.

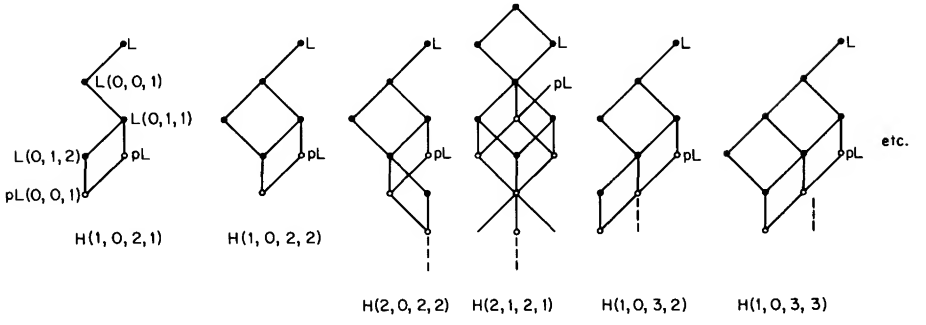


FIG. 5

4.

We want to make some comments on the behavior of centerings if one replaces the Dedekind domain R by a Dedekind domain R' containing R such that the quotient field K' of R' is a finite field extension of K. Let $H' = R' \otimes_R H$ and $L' = R' \otimes_R L$ for any H-representation module L. In Zassenhaus and Reiner [18] it is proved that $L_1' \cong L_2'$ iff $L_1 \cong L_2$, in case R is local. If L is absolutely irreducible, a somewhat more precise description of the situation can be given.

Theorem 4.1 *Let L be absolutely irreducible.*

(i) [18] *The mapping* $\mathfrak{Z}(L) \to \mathfrak{Z}(L')$: $M \to R' \otimes M = M'$ *is injective.* $\mathfrak{R}(L)$ *is mapped into* $\mathfrak{R}(L')$.

(ii) *Let* $\mathfrak{P}$ *be a (critical) prime ideal of* R *and let the* $\mathfrak{P}$*-centerings of* $\mathfrak{R}(L)$ *all contain* $\mathfrak{P}^\alpha L$. *Let* $\mathfrak{P}'$ *be an unramified prime ideal of* R' *dividing* $\mathfrak{P}$. *The mapping* Φ: $\mathfrak{Z}_{\mathfrak{P}}(L) \cap \mathfrak{R}(L) \to \mathfrak{Z}_{\mathfrak{P}'}(L')$: $M \to M' + \mathfrak{P}^\alpha L'$ *is injective. Assume that the constituents of* $L/\mathfrak{P}L$ *are absolutely irreducible.* Φ *is a bijection if and only if* $R/\mathfrak{P} \cong R'/\mathfrak{P}'$ *or if the lattice* $\mathfrak{Z}_{\mathfrak{P}}(L)$ *of* $\mathfrak{P}$*-centerings of* L *is distributive.*

Proof (i) Let $M, N \in \mathfrak{Z}(L)$ with $M' = N'$. Choose $r \in R$ such that $rM \subseteq N$ and denote the invariant factor ideals of rM in N by $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$. Then $(rM)' = rM' \subseteq N'$ with invariant factor ideals $\mathfrak{A}_1 R', \ldots, \mathfrak{A}_n R'$. Part (i) now follows easily.

(ii) The injectivity of Φ follows from the proof of part (i) of this theorem and from Proposition 2.6. To prove the last statement we first note that the maximal $\mathfrak{P}'$-centerings correspond to certain one-dimensional subspaces of certain $R'/\mathfrak{P}'$-vector spaces of homomorphisms as described in Lemma 3.7.

The maximal $\mathfrak{P}$-centerings of M correspond to the one-dimensional subspaces of the corresponding $R/\mathfrak{P}$-vector spaces from which the $R'/\mathfrak{P}'$-spaces under consideration can be obtained by tensoring with $R'/\mathfrak{P}'$. Now it is easy to see that the $R'/\mathfrak{P}'$-subspaces are in one-to-one correspondence with the $R/\mathfrak{P}$-subspaces iff $R/\mathfrak{P} = R'/\mathfrak{P}'$ or if all the spaces are one dimensional, i.e., the lattice of $\mathfrak{P}$-centerings is distributive. QED

Corollary 4.2 *If under the assumption of Theorem* 4.1 $\mathfrak{P}'$ *is ramified with ramification index* a, *then the number of* $\mathfrak{P}'$*-centerings in* $\mathfrak{R}(L')$ *is greater than or equal to*

$$a \cdot (\textit{number of } \mathfrak{P}\textit{-centerings in } \mathfrak{R}(L) - 1) + 1$$

and the critical $\mathfrak{P}'$*-exponent of* L' *is greater or equal to*

$$a \cdot (\textit{critical } \mathfrak{P}\textit{-exponent of } L).$$

If $M \in \mathfrak{Z}_{\mathfrak{P}}(L) \cap \mathfrak{R}(L)$ *such that no proper centering of* M *has this property, then* M' *is also minimal in* $\mathfrak{Z}_{\mathfrak{P}'}(L') \cap \mathfrak{R}(L')$.

Proof The last statement follows immediately from Theorem 4.1 (ii) and the definition of $\mathfrak{R}(L)$. To prove the first result let $M, N \in \mathfrak{Z}_{\mathfrak{P}}(L)$ with $M \subset N$ maximal and let $R_{\mathfrak{P}} = (\mathfrak{B}')^a\mathfrak{U}$. Then

$$N'/M' \supset \mathfrak{P}'(N'/M') \supset \cdots \supset (\mathfrak{P}')^a(N'/M')$$

where all inclusions are proper. The inverse images of these modules are different $\mathfrak{P}'$-centerings of L'.

The result follows now from Proposition 2.6 and an easy counting argument. QED

Distributivity of lattices of centerings is not always preserved under ramified extensions if the projective composition factors are not in one-to-one correspondence with the (usual) composition factors. For example, the dihedral group of eight elements has an irreducible $\mathbb{Z}$-representation of degree 2. The lattice of 2-centerings is linearly ordered and the constituents of $L/2L$ are the 1-constituents. (D_8 is a 2-group!) By taking this representation over the gaussian integers $\mathbb{Z}[i]$, the lattice of $(1 + i)$-centerings becomes nondistributive (Fig. 6). By Corollary 3.8 there are three maximal (H_i)-centerings of $M' + (1 + i)L'$. Hence $\mathfrak{Z}_{(1+i)}(L')$ is not distributive.

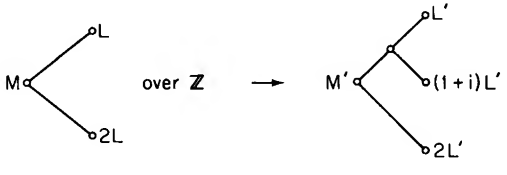


FIG. 6

5.

We want to consider some examples of absolutely irreducible $\mathbb{Z}G$-representations, where G is a finite group.

Let G be a 2-transitive permutation group of $\Omega = \{1, \ldots, n\}$. Let $I = \bigoplus_{i=1}^{n} \mathbb{Z}E_i$ be the representation module of the permutation representation, i.e., $gE_i = E_{g(i)}$ for $g \in G$ and $i \in \Omega$. The factor module $L = I/\mathbb{Z}\sum_{i=1}^{n} E_i$ is an absolutely irreducible representation module by Burnside's lemma [8]. Denote the coset of E_i by e_i. In case $G = S_n$, the constituents of the factor modules L/pL are well known [6] for all primes p:

(a) L/pL is irreducible for $p \nmid n$.

(b) L/pL has two constituent for $p \mid n$. (One of the constituents is the 1-constituent.)

In [9] it is proved that (a) and (b) also hold for $G = A_n$ or certain of the Mathieu groups.

Theorem 5.1 *Let G be a 2-transitive permutation group such that* (a) *and* (b) *hold (for instance $G = S_n$, A_n). Then the set of representatives $\mathfrak{R}(L)$ consists of all centerings L_d of L for $d \mid n$, where*

$$L_d = \{\textstyle\sum_{i=1}^{n+1} \alpha_i e_i \mid d \text{ divides } \sum_{i=1}^{n} \alpha_i\}.$$

The index of L_d in L is d. Hence the class number of L is the number of the divisor of n.

Proof Because of (a) there are no p-centerings for $p \nmid n$. Let G act trivially on $\mathbb{Z}/n\mathbb{Z}$. Then $L_n = \ker \varphi$ with $\varphi: L \to \mathbb{Z}/n\mathbb{Z}$ via $\sum_{i=1}^{n} \alpha_i e_i \to \sum_{i=1}^{n} \bar{\alpha}_i$. φ is well defined because of $\sum_{i=1}^{n} e_i = 0$ and is a $\mathbb{Z}G$-homomorphism. For $d \mid n$, we get L_d as the inverse image of $d \cdot (\mathbb{Z}/n\mathbb{Z})$ under φ. Hence the invariant factors of L_d in L are

$$\underbrace{1, \ldots, 1}_{n-2}, d.$$

So $L_d \in \mathfrak{R}(L)$. To show that there are no other centerings in $\mathfrak{R}(L)$ we make use of (b) and apply Theorem 3.22. We only have to show that L/pL and (applying Proposition 2.6) L_n/pL_n are indecomposable for $p \mid n$. So let $g\sum_{i=1}^{n} \alpha_i e_i \equiv \sum_{i=1}^{n} \alpha_i e_i \pmod{p}$, hence

$$\alpha_{g(1)} - \alpha_1 \equiv \cdots \equiv \alpha_{g(n)} - \alpha_n \pmod{p}$$

for all $g \in G$. By using the 2-transitivity of G, one gets $\alpha_1 \equiv \alpha_2 \equiv \cdots \equiv \alpha_n \pmod{p}$, hence $\sum_{i=1}^{n} \alpha_i e_i \equiv 0 \pmod{pL}$, i.e., L/pL is indecomposable. The indecomposability of L_n/pL_n follows immediately from the observation that the modules L and L_n are dual (via the quadratic form of L fixed by G). We

indicate another proof: L_n is generated by $e_i - e_j$ $(i, j = 1, \ldots, n, i \neq j)$. Let $\varphi: L_n \to \mathbb{Z}/p\mathbb{Z}$ be a $\mathbb{Z}G$-homomorphism, where G acts trivially on $\mathbb{Z}/p\mathbb{Z}$. Because of the 2-transitivity of G all $e_i - e_j$ are mapped on the same element of $\mathbb{Z}/p\mathbb{Z}$. For odd p this implies immediately $\varphi = 0$ because $\varphi(e_i - e_j) = \varphi(e_j - e_i)$. If $p = 2$, one gets $3\varphi(e_i - e_j) = \varphi(e_i - e_j) = 0$ from $(e_1 - e_2) + (e_2 - e_3) + (e_3 - e_1) = 0$. Hence $\varphi = 0$ and L_n/pL_n is also indecomposable. QED

For $G = S_n$, Theorem 5.1 was already stated without proof in [7]. A similar proof as above can be found in [11] also for $G = S_n$.

For our next example let G be an irreducible subgroup of $GL(n, \mathbb{Z})$ containing all the diagonal matrices of $GL(n, \mathbb{Z})$. It is clear that G is a semidirect product of the elementary abelian 2-group D_n of all diagonal matrices of $GL(n, \mathbb{Z})$ of order 2^n and a transive group P_n of permutation matrices of degree n.

Theorem 5.2 *Let $G = D_n P_n$ as described above and $L = \mathbb{Z}^{n \times 1}$. Then all centerings of $\mathfrak{R}(L)$ lie between L and $2L$ and are in one-to-one correspondence with the normal subgroups of G contained in D_n and unequal* 1.

Proof Let $e_1, \ldots, e_n$ be the standard basis of L and let e_{ij} $(i, j = 1, \ldots, n)$ be the matrix units of $\mathbb{Z}^{n \times n}$ with $e_{ij} e_k = \delta_{jk} e_i$. We want to show that $2e_{ij}$ are contained in the ($\mathbb{Z}$-)enveloping algebra $\phi(G)$ of G. Let $g \in P_n$ with $ge_i = e_j$. Then

$$g - \operatorname{diag}(1, \ldots, 1, \underset{\substack{\uparrow \\ j}}{-1}, 1, \ldots, 1)g = 2e_{ij} \in \phi(G).$$

Hence the last invariant factor of $\phi(G)$ in $\mathbb{Z}^{n \times n}$ is 2. By Theorem 2.7 all centerings of $\mathfrak{R}(L)$ lie between L and $2L$. One easily sees now that D_n and $L/2L$ are equivalent G-modules where G acts on D_n by conjugation. QED

Corollary 5.3 *If P_n in Theorem* 5.2 *is cyclic, the centerings of L in $\mathfrak{R}(L)$ are in one-to-one correspondence with the divisors $\neq 1$ of $(x^n - 1)$ in $\mathbb{Z}/2\mathbb{Z}[x]$.*

Corollary 5.4 *If P_n in Theorem* 5.2 *satisfies the conditions* (a) *and* (b) *at the beginning of this section, then the class number is three. The centerings of $L = \mathbb{Z}^{n \times 1}$ in $\mathfrak{R}(L)$ are L, $N = \{\sum_{i=1}^n \alpha_i e_i \mid 2$ divides $\sum_{i=1}^n \alpha_i\}$ and $M = \{\sum_{i=1}^n \alpha_i e_i \mid \alpha_i \equiv \alpha_j \pmod 2$ for $i, j = 1, \ldots, n\}$.*

Note that for even n the 2-centerings of L in (5.4) are linearly ordered: $L \supset N \supset M \supset 2L \cdots$. L/N and $M/2L$ are 1-constituents. This is an example that projective constituents and ordinary constituents differ from each other.

As a further example we mention that it is proved by Zassenhaus [15] that for absolutely irreducible representation modules L of metacyclic groups the lattice of p-centerings is linearly ordered and the p-centerings of

$\mathfrak{R}(L)$ lie between L and pL. (It is proved that $\phi_L(G)$ is a hereditary order.)

As a last example we take the 2-group of 8×8 matrices given by

$$\left\langle \begin{bmatrix} A & 0 & 0 & 0 \\ 0 & A & 0 & 0 \\ 0 & 0 & A & 0 \\ 0 & 0 & 0 & A \end{bmatrix}, \begin{bmatrix} 0 & I_2 & 0 & \\ B & 0 & & \\ & & 0 & I_2 \\ 0 & & B & 0 \end{bmatrix}, \begin{bmatrix} 0 & I_4 \\ I_4 & 0 \end{bmatrix} \right\rangle$$

where $A = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$. Note that by Theorem 2.8 the only nontrivial centerings of $L = \mathbb{Z}^{8\times 1}$ are 2-centerings and that for p-groups there is only one modular irreducible representation. The centerings in this example were computed electronically by M. Pohst and myself by using the program written for Plesken and Pohst [12]. The lattice of 2-centerings is shown in Fig. 7. The class number is 32. But one can easily construct examples of 2-groups of degree 8 with higher class numbers.

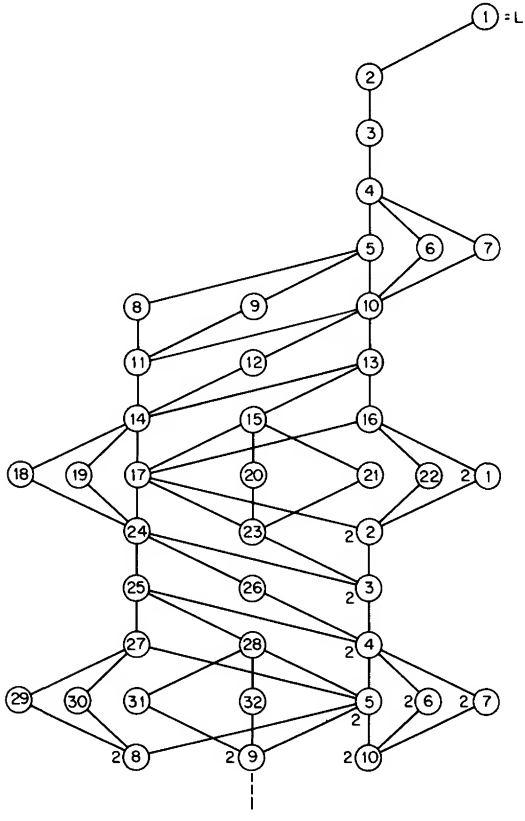


FIG. 7

REFERENCES

[1] G. Birkhoff, "Lattice Theory" (AMS Colloq. Publ. **25**). Amer. Math. Soc., Providence, Rhode Island, 19 .

[2] R. Brauer, Investigations on group characters, *Ann. Math.* **42** (1941), 937–958.

[3] R. Brauer and C. Nesbitt, On the modular characters of groups, *Ann. Math.* **42** (1941), 556–590.

[4] R. Brauer and C. Nesbitt, On the modular representation of groups of finite order, I. Univ. of Toronto Studies, Math. Series No. 4, 1937.

[5] W. C. Curtis and I. Reiner, "Representation Theory of Finite Groups and Associative Algebras." Wiley (Interscience), New York, 1962.

[6] H. K. Farahat, On the natural representation of symmetric groups, *Proc. Glasgow Math. Assoc.* **5** (1962), 121–136.

[7] C. Hermann, "Translationsgruppen in n Dimensionen, Zur Struktur und Materie der Festkörper, pp. 24–33. Springer-Verlag, Berlin–Göttingen–Heidelberg, 1951.

[8] B. Huppert, "Endliche Gruppen," Vol. I. Springer-Verlag, Berlin–Heidelberg–New York, 1967.

[9] M. Klemm, Über die Reduktion von Permutationsmoduln, *Math. Z.* **143** (1975), 113–117.

[10] J. M. Maranda, On the equivalence of representations of finite groups by groups of automorphisms of modules over Dedekind rings, *Can. J. Math.* **7** (1955), 516–526.

[11] W. Plesken, Beiträge zur Bestimmung der endlichen irreduziblen Untergruppen von $GL(n, \mathbb{Z})$, Dissertation, Aachen, 1974.

[12] W. Plesken and M. Pohst, On maximal finite irreducible subgroups of $GL(n, \mathbb{Z})$: I, The five and seven dimensional case; II, The six dimensional case, to appear.

[13] I. Schur, "Über Gruppen linearer Substitutionen mit Koefficienten aus einem algebraischen Zahlkörper," Gesammelte Abhandlungen, Bd. 1, pp. 451–463. Springer-Verlag, Berlin–Heidelberg–New York,

[14] H. Zassenhaus, Graduated orders, manuscript.

[15] H. Zassenhaus, Crossed product orders, to appear.

[16] H. Zassenhaus, Neuer Beweis der Endlichkeit der Klassenzahl bei unimodularer Äquivalenz endlicher ganzzahliger Substitutionsgruppen, *Abh. Math. Sem. Univ. Hamburg* **12** (1938), 276–288.

[17] H. Zassenhaus, A condition for compatibility of submodules of a module, *J. Number Theory* **1** (1969), 467–476.

[18] H. Zassenhaus and I. Reiner, Equivalence of representations under extensions of local ground rings, *Ill. J. Math.* **5** (1961), 409–411.

AMS (MOS) 1970 subject classifications: 16A18, 16A64, 20C10.

The Existence of P-adic Abelian L-functions

CARY QUEEN†

UNIVERSITY OF CALIFORNIA
BERKELEY, CALIFORNIA

We first prove that a modular form on $\Gamma_0(p^r)$, $r \geq 1$, is a p-adic modular form. Using this fact, we establish the existence of a p-adic L-function for each abelian character of any totally real number field.

Introduction

It is a well-known but remarkable fact that the values of the Riemann zeta function at negative integers are rational. This phenomenon suggested to Kubota and Leopoldt the possibility of defining a "p-adic zeta function" on $\mathbf{Z}_p$ by p-adic interpolation between these values [6]. More generally, they proved that for every Dirichlet character χ, there is a continuous p-adic L-function $L_p(\chi, s)$ on $\mathbf{Z}_p$ such that $L_p(\chi, 1-n) = L(\chi, 1-n)$ for positive integers $n \equiv 0 \bmod(p-1)$. The significance of this result was enhanced by Iwasawa's later discovery of the connection between p-adic L-functions and cyclotomic extensions [3].

It would naturally be of interest to extend the concept of p-adic L-functions to any algebraic number field. This might be possible for at least

† Present address: Department of Mathematics, Cornell University, Ithaca, New York.

totally real number fields because then $L_K(\chi, 1-n)$ is an algebraic number [5], not always zero. However, the project has been stymied by the lack of congruences for $L_K(\chi, 1-n)$ analogous to those for $L_{\mathbf{Q}}(1, 1-n) = -B_n/n$. Coates and Sinnott did recently treat real quadratic K using an explicit formula of Siegel [2].

J.-P. Serre created a new approach to the question when he introduced the concept of "p-adic modular form" [10]. Siegel had earlier noticed that $L_K(\chi, 1-n)$ is the constant term of a modular form. Serre's $L_p(\chi, 1-s)$ turns out to be the constant term of a *p-adic* modular form. However, because he relied on a theorem that modular forms on $\Gamma_0(p)$ are p-adic modular forms, Serre's treatment was limited to characters of extensions $K(\zeta_p)/K$.

The object of the present paper is to prove the existence of a p-adic L-function associated to any abelian character χ of any totally real number field. The basic tool in our proof is a theorem that any modular form on $\Gamma_0(p^r)$, $r \geq 1$, is a p-adic modular form.† In order to be fully general, everything must be done in the setting of p-adic modular forms of level N, a generalization of Serre's original idea due to Katz [4].

In Section 1 some results of Katz are rapidly redone in the style of Serre in order to provide a convenient starting point for the present work.

In Section 2 the idea of a p-adic modular quasiform is introduced. This technical notion is precisely what is needed to prove our basic theorems. The proofs in this section are just slight variations of proofs of Serre [9, 10], but the results seem genuinely stronger.

In Section 3 we show directly that certain modular forms on a group "$\Gamma_{01}(p^2)$" are p-adic modular quasiforms. These forms are then used to show inductively that modular forms of level N on $\Gamma_0(p^r)$ are p-adic modular forms of level N.

In Section 4 the previous results are extended to modular forms on $\Gamma_1(p^r)$ having characters with respect to $\Gamma_0(p^r)$. In particular, it is shown that the higher the conductor of the character, the more rigidly is the constant term determined.

Finally, we present a proof of the existence of p-adic abelian L-functions and discuss their continuity at $s = 1$.

I would like to thank J. Coates, N. Katz, J.-P. Serre, and especially my advisor A. Ogg for help and encouragement.

1. Preliminaries

For any prime p, let Ω_p denote an algebraic closure of $\mathbf{Q}_p$, so Ω_p is a compositum of the field of p-adic numbers $\mathbf{Q}_p$ and the field of algebraic

† We have been informed that N. Katz has also obtained this result.

numbers $\bar{\mathbf{Q}}$. Fix once and for all an extension v_p of the p-adic valuation to Ω_p, normalized so $v_p(p) = 1$. If K is an extension of $\mathbf{Q}$ in $\bar{\mathbf{Q}}$, let $\mathcal{O}_K$ be its ring of integers and $\tilde{K}$ its residue field. Should K be finite over $\mathbf{Q}$, write $K_p = K\mathbf{Q}_p$ for its closure in Ω_p.

Let G be any subgroup of $\Gamma = SL(2, \mathbf{Z})$ which contains $\left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)$, and put $q = e^{2\pi iz/N}$. A modular form f on G is said to be defined over K if the q-expansion of f at $i\infty$ is $\sum_{n=0}^{\infty} a_n q^n$ with each $a_n \in K$. If in fact f is defined over $\mathcal{O}_K$, i.e., each $a_n \in \mathcal{O}_K$, then $\tilde{f} = \sum_{n=0}^{\infty} \tilde{a}_n q^n \in \tilde{K}[[q]]$ is called the reduction of f. Denote by $\mathcal{M}_K(G, k)$ the vector space over K of (holomorphic) modular forms on G of weight k defined over K, and by $\tilde{\mathcal{M}}_K(G, k)$ the $\tilde{K}$-subspace of $\tilde{K}[[q]]$ consisting of the reductions of all forms in $\mathcal{M}_K(G, k)$ defined over $\mathcal{O}_K$. Finally, let $\mathcal{M}_K(G)$ be the subalgebra $\sum_{k=0}^{\infty} \mathcal{M}_K(G, k)$ of $K[[q]]$ and $\tilde{\mathcal{M}}_K(G)$ the corresponding subalgebra $\sum_{k=0}^{\infty} \tilde{\mathcal{M}}_K(G, k)$ of $\tilde{K}[[q]]$. For short, $\mathcal{M}_{\bar{\mathbf{Q}}}(G, k)$ will be abbreviated by $\mathcal{M}(G, k)$, $\tilde{\mathcal{M}}_{\bar{\mathbf{Q}}}(G)$ by $\tilde{\mathcal{M}}(G)$, and so on. We take as our starting point two fundamental theorems.

Theorem A (Swinnerton-Dyer) *If $p \neq 2, 3$, then*

$$\tilde{\mathcal{M}}(\Gamma) \simeq \bar{\mathbf{F}}_p[Q, R]/(\tilde{A} - 1)$$

where Q and R are indeterminates and $A(Q, R)$ is the polynomial such that $E_{p-1} = A(E_4, E_6)$. If $p = 2$ or 3, then $\tilde{\mathcal{M}}(\Gamma) \simeq \bar{\mathbf{F}}_p[\tilde{\Delta}]$ with $\tilde{\Delta}$ algebraically independent over $\bar{\mathbf{F}}_p$.

We write $v_p(\sum_{n=0}^{\infty} a_n q^n)$ for $\inf_{n \geq 0} v_p(a_n)$ and $\{x\}$ for the least integer greater than or equal to x.

Theorem B (Serre, Katz) *Let $f^{(1)} = \sum_{n=0}^{\infty} a_n^{(1)} q^n$ and $f^{(2)} = \sum_{n=0}^{\infty} a_n^{(2)} q^n$ be members of $\mathcal{M}(\Gamma(N), k_1)$ and $\mathcal{M}(\Gamma(N), k_2)$ respectively. Suppose $r \in \mathbf{Q}$, $(p, N) = 1$, and $v_p(f^{(1)} - f^{(2)}) \geq v_p(f^{(1)}) + r$. Then:*

(1) *if $p \neq 2$ and $r > 0$, $k_1 \equiv k_2 \bmod (p-1)p^{\{r\}-1}$;*
(2) *if $p = 2$ and $r > 1$, $k_1 \equiv k_2 \bmod 2^{\{r\}-2}$.*

The proof of Theorem A is the same, *mutatis mutandis*, as the proof of Theorem 2 in [12], with $\bar{\mathbf{Q}}$ replacing $\mathbf{Q}$ and $\bar{\mathbf{F}}_p$ replacing $\mathbf{F}_p$.

To prove Theorem B, we may assume that $v_p(f^{(1)}) = 0$ after multiplying $f^{(1)}$ and $f^{(2)}$ by an appropriate constant. Suppose $f^{(1)}$ and $f^{(2)}$ are defined over a number field L with maximal unramified subfield K, so $\tilde{K} = \tilde{L}$ and $\mathcal{O}_{K_p}$ is the Witt ring $W(\tilde{K})$. Let $w_1, \ldots, w_n$ be an integral basis for L_p over K_p, i.e., a basis for the module $\mathcal{O}_{L_p}$ over the ring $\mathcal{O}_{K_p}$. Since $\mathcal{M}(\Gamma(N), k)$ always has a basis of forms defined over $\mathbf{Q}$, there are K_p-linear combinations $f_j^{(i)}$ of modular forms over $\mathbf{Q}$ such that $f^{(1)} = \sum_j w_j f_j^{(1)}$ and $f^{(2)} = \sum_j w_j f_j^{(2)}$. Choose $\hat{w}_j \in K_p$ such that $\tilde{\hat{w}} = \tilde{w}_j$, so for each j, $v_p(\hat{w}_j - w_j) > 0$ and $v_p(f_j^{(1)} - f_j^{(2)}) \geq [r]$. As an easy consequence, if $\hat{f}^{(i)} = \sum_j \hat{w}_j f_j^{(i)}$, then $v_p(\hat{f}^{(1)} - \hat{f}^{(2)}) \geq [r]$ for $[r] = r$ and $v_p(\hat{f}^{(1)} - \hat{f}^{(2)}) > [r]$ for $[r] \neq r$. Since

$\hat{f}^{(1)} - \hat{f}^{(2)}$ is defined over the unramified field K_p, in either case $v_p(f^{(1)} - f^{(2)}) \geq \{r\}$. The theorem now follows by applying Corollary 4.4.2 of [4] to $\hat{f}^{(i)} \in S(W(\bar{K}), 1, N, k_i)$.

In all that follows, by a limit of a sequence of series $f^{(i)} = \sum_{n=0}^{\infty} a_n^{(i)} q^n$, $a_n^{(i)} \in \Omega_p$, we shall mean a series $f = \sum_{n=0}^{\infty} a_n q^n$ such that $\lim_{i \to \infty} a_n^{(i)} = a_n$ uniformly for all n. Moreover, p will always denote a prime not dividing a fixed positive integer N, and K will denote some *finite* extension of $\mathbf{Q}$. By a *p-adic modular form f over K of level N*, we mean a limit of a sequence $f^{(i)} \in \mathcal{M}_K(\Gamma(N), k_i)$. It follows immediately from Theorem B that the k_i approach a limit k in $X = \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$, which is independent of the particular sequence of modular forms $f^{(i)}$ approaching f and is called the weight of f. The set of p-adic modular forms over K of level N and weight k is a K_p-vector space $\bar{\mathcal{M}}_K(\Gamma(N), k)$ closed under limits. Moreover, the p-adic modular forms of level N and weight k over *all* finite extensions of $\mathbf{Q}$ constitute a vector space over Ω_p, denoted $\bar{\mathcal{M}}(\Gamma(N), k)$. Any member of $\bar{\mathcal{M}}(\Gamma(N), k)$ can be called a p-adic modular form of level N, without regard to its particular field of definition, and p-adic modular forms of level 1 can simply be called p-adic modular forms.

Two important corollaries may be deduced from Theorem B.

Corollary C *Let* $f = \sum_{n=0}^{\infty} a_n q^n \in \bar{\mathcal{M}}(\Gamma(N), k)$ *with* $k = (t, s) \in \mathbf{Z}_p \times \mathbf{Z}/(p-1)\mathbf{Z}$. *Then:*

(1) *if* $s \neq 0$, $v_p(a_0) \geq \inf_{n \geq 1} a_n$;
(2) *if* $s = 0$, $v_p(a_0) \geq \inf_{n \geq 1} a_n - v_p(t) - 1 - \delta_{2,p}$.

Corollary D *Let* $f^{(i)} = \sum_{n=0}^{\infty} a_n^{(i)} q^n \in \bar{\mathcal{M}}_K(\Gamma(N), k_i)$; $i = 1, 2, \ldots$. *Suppose that the* $a_n^{(i)}$ *tend uniformly toward* $a_n \in \Omega_p$ *for* $n \geq 1$, *and the* k_i *approach a nonzero limit* k *in* X. *Then the* $a_0^{(i)}$ *have a limit* $a_0 \in \Omega_p$, *and* $f = \sum_{n=0}^{\infty} a_n q^n \in \bar{\mathcal{M}}_K(\Gamma(N), k)$.

Corollary C follows directly from Theorem B upon approximating f by $f^{(1)} \in \mathcal{M}(\Gamma(N), \hat{t})$, letting $f^{(2)} = a_0 \in \mathcal{M}(\Gamma(N), 0)$, and observing that $v_p(f^{(1)} - f^{(2)}) = \inf_{n \geq 1} v_p(a_n)$. For the proof of Corollary D, first recall that the Eisenstein series $E_k \equiv 1 \bmod p^m$ if $k \equiv 0 \bmod (p-1)p^{m-1}$ $(p \neq 2)$ and $E_k \equiv 1 \bmod 2^m$ if $k \equiv 0 \bmod 2^{m-2}$. Since K is a finite extension of $\mathbf{Q}$, K_p is complete. To show that the $a_0^{(i)}$ converge, it therefore suffices to show that they form a Cauchy sequence. Since $\lim_{i \to \infty} k_i = k = (t, s) \neq 0$, either $s \neq 0$ and $k_i \neq 0 \bmod (p-1)$ for i large enough, or $t \neq 0$ and $v_p(k_i)$ is bounded. By Corollary C, the $v_p(a_0^{(i)})$ are thus bounded, and upon multiplying all the $f^{(i)}$ by a constant, one may assume that $v_p(f^{(i)}) \geq 0$ for each i. By assumption, if i_1 and i_2 are large enough, $\inf_{n \geq 1} v_p(a_n^{(i_2)} - a_n^{(i_1)}) \geq M$ and $k_{i_2} \equiv k_{i_1} \bmod (p-1)p^{M-1}$ for given M. If $k_{i_2} > k_{i_1}$, say, then Corollary C applied to $f^{(i_2)} - E_{k_{i_1} - k_{i_2}} f^{(i_1)} \in \bar{\mathcal{M}}(\Gamma(N), k_{i_2})$ yields $v_p(a_0^{(i_2)} - a_0^{(i_1)}) \geq M$ if

$k_{i_2} \not\equiv 0 \bmod(p-1)$ and $v_p(a_0^{(i_2)} - a_0^{(i_1)}) \geq M - v_p(k_{i_2}) - 2$ if $k_{i_2} \equiv 0$, as desired. Finally, $f \in \bar{\mathcal{M}}_K(\Gamma(N), k)$ by the definition of p-adic modular forms over K of level N and weight k.

Our first two propositions show that no essentially new reduced or p-adic modular forms arise when the field of definition is extended. Consequently, a reduced or p-adic modular form is defined over K precisely when its coefficients are all contained in $\tilde{K}$ or K_p.

Proposition 1 $\bar{\mathcal{M}}_K(\Gamma(N), k) = \bar{\mathcal{M}}_{\mathbf{Q}}(\Gamma(N), k) \otimes_{\mathbf{Q}} \tilde{K}$.

Proof Let $w_1, \ldots, w_n$ be an integral basis for K_p over $\mathbf{Q}_p$. If $\tilde{f} \in \bar{\mathcal{M}}_K(\Gamma(N), k)$, let $f \in \mathcal{M}_K(\Gamma(N), k)$ have reduction $\tilde{f}$. Then $f = \sum_j w_j f_j$ with $f_j \in \mathcal{O}_{K_p}[[q]]$ a $\mathbf{Q}_p$-linear combination of members of $\mathcal{M}_{\mathbf{Q}}(\Gamma(N), k)$. Since each f_j may be approximated by a member of $\mathcal{M}_{\mathbf{Q}}(\Gamma(N), k)$, $\tilde{f}_j \in \bar{\mathcal{M}}_{\mathbf{Q}}(\Gamma(N), k)$ and $\tilde{f} = \sum_j \tilde{w}_j \tilde{f}_j \in \bar{\mathcal{M}}_{\mathbf{Q}}(\Gamma(N), k) \otimes_{\mathbf{Q}} \tilde{K}$.

Corollary *If* $\tilde{f} = \sum_{n=0}^{\infty} a_n q^n \in \bar{\mathcal{M}}(\Gamma(N), k)$, *then* $\tilde{f} \in \bar{\mathcal{M}}_K(\Gamma(N), k)$ *if and only if each* $a_n \in \tilde{K}$.

Proof Only the "if" assertion requires proof. By the proposition, $\tilde{f} = \sum_j c_j \tilde{f}_j$ with $\tilde{f}_j \in \bar{\mathcal{M}}_{\mathbf{Q}}(\Gamma(N), k)$ linearly independent and $c_j \in \bar{\mathbf{F}}_p$. Since $\tilde{f}$ and the $\tilde{f}_j$ have all coefficients in $\tilde{K}$, the c_j are also contained in $\tilde{K}$, say by Cramer's rule, so $\tilde{f} \in \bar{\mathcal{M}}_K(\Gamma(N), k)$ as desired.

Proposition 2 $\bar{\mathcal{M}}_K(\Gamma(N), k) = \bar{\mathcal{M}}_{\mathbf{Q}}(\Gamma(N), k) \otimes_{\mathbf{Q}p} K_p = \bar{\mathcal{M}}_{\mathbf{Q}}(\Gamma(N), k) \otimes_{\mathbf{Q}} K$.

Proof It is enough to show that if $f = \lim_{i \to \infty} f^{(i)}$ with $f^{(i)} \in \mathcal{M}_K(\Gamma(N), k_i)$, then f is a K_p-linear combination of members of $\bar{\mathcal{M}}_{\mathbf{Q}}(\Gamma(N), k)$. Let $w_1, \ldots, w_n$ be a basis for K_p over $\mathbf{Q}_p$ and write $f = \sum_j f_j w_j, f^{(i)} = \sum f_j^{(i)} w_j$, where the f_j and $f_j^{(i)}$ have coefficients in $\mathbf{Q}_p$. The $f_j^{(i)}$ are $\mathbf{Q}_p$-linear combinations of modular forms over $\mathbf{Q}$, hence elements of $\bar{\mathcal{M}}_{\mathbf{Q}}(\Gamma(N), k_i)$. Recall that the norm defined by $\| \sum_j \alpha_j w_j \| = \sum_j |\alpha_j|_p$ is equivalent to the v_p-norm on K_p. Thus $\sum_j f_j^{(i)} w_j \to \sum_j f_j w_j$ forces $f_j^{(i)}$ to approach f_j for each j, that is, $f_j \in \bar{\mathcal{M}}_{\mathbf{Q}}(\Gamma(N), k)$ and $f = \sum_j f_j w_j \in \bar{\mathcal{M}}_{\mathbf{Q}}(\Gamma(N), k) \otimes K_p$.

Corollary 1 *If* $f = \sum_{n=0}^{\infty} a_n q^n \in \bar{\mathcal{M}}(\Gamma(N), k)$, *then* $f \in \bar{\mathcal{M}}_K(\Gamma(N), k)$ *if and only if each* $a_n \in K$.

Corollary 2 *A p-adic modular form with coefficients in* $\mathbf{Q}_p$ *is a p-adic modular form in the sense of Serre.*

Proof Corollary 1 is proved in the same manner as the corollary to Proposition 2, and Corollary 2 is of course a special case of Corollary 1.

Consider the linear operators $U, V: \Omega_p[[q]] \to \Omega_p[[q]]$ defined by

$$\sum_{n=0}^{\infty} a_n q^n \,|\, U = \sum_{n=0}^{\infty} a_{pn} q^n \qquad \text{and} \qquad \sum_{n=0}^{\infty} a_n q^n \,|\, V = \sum_{n=0}^{\infty} a_n q^{pn}.$$

Proposition 3 *If* $f = \sum_{n=0}^{\infty} a_n q^n \in \bar{\mathcal{M}}_K(\Gamma(N), k)$, *then*

$$f \mid U, f \mid V \in \bar{\mathcal{M}}_K(\Gamma(N), k).$$

Proof By Corollary 2.1, it suffices to show that U and V map $\bar{\mathcal{M}}(\Gamma(N), k)$ into itself. Since U and V commute with limits, this would follow if U and V mapped $\mathcal{M}(\Gamma(N), k)$ into $\bar{\mathcal{M}}(\Gamma(N), k)$ for $k \in \mathbf{Z}$. There is a decomposition

$$\mathcal{M}(\Gamma(N), k) = \bigoplus_{\chi \in (\mathbf{Z}/N\mathbf{Z})^{x^*}} \mathcal{M}(\Gamma(N), \chi, k)$$

where

$$\mathcal{M}(\Gamma(N), \chi, k) = \left\{ f \in \mathcal{M}(\Gamma(N), k) \mid f|_k \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \chi(d) f \right.$$

$$\left. \text{for } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma,\ b \equiv c \equiv 0 \bmod N \right\}.$$

Hence, all one needs is $f \mid U, f \mid V \in \bar{\mathcal{M}}(\Gamma(N), k)$ for $f \in \mathcal{M}(\Gamma(N), \chi, k)$. Write $k_m = (p-1)p^{m-1}$ and $f_m = E_{k_m} f \in \mathcal{M}(\Gamma(N), \chi, k + k_m)$, so $k_m \to 0$ and $f_m \to f$ as $m \to \infty$. By the theory of Hecke operators, $f_m \mid T_p = f_m \mid U + \chi(p) p^{k+k_m-1} f_m \mid V \in \mathcal{M}(\Gamma(N), k + k_m)$. Therefore

$$f \mid U = \lim f_m \mid U = \lim f_m \mid T_p \in \mathcal{M}(\Gamma(N), k),$$

completing the proof for U. In particular, $f_m \mid V = \bar{\chi}(p) p^{1-k_m-k}(f_m \mid T_p - f_m \mid U) \in \mathcal{M}(\Gamma(N), k + k_m)$ and $f \mid V = \lim f_m \mid V \in \mathcal{M}(\Gamma(N), k)$, completing the proof for V.

In [10], Serre shows that general Hecke operators T_l and differential operators Θ and R_h, as well as U and V, preserve p-adic modular forms of level 1. As Serre has pointed out to us, Θ and R_h also preserve p-adic modular forms of level N. For it follows from the transformation formula for E_2 that if f is a modular form on any subgroup of Γ, in particular $\Gamma(N)$, then so is $\Theta f - (\text{wt } f/12) E_2 f$, while $E_2 \in \bar{\mathcal{M}}(\Gamma, 2)$. The situation for the T_l is more complicated, however.

2. *p*-adic Modular Quasiforms

For later purposes, a version of Corollary D will be needed which applies to certain *sums* of p-adic modular forms. As a first step in this direction, we define the relevant sums precisely.

Definition $f = \sum_{n=0}^{\infty} a_n q^n \in \Omega_p[[q]]$ is a p-adic modular quasiform over K of level N and weight $k \in \mathbf{Z}_p$ if $f = \sum_{\alpha=1}^{p-1} f_\alpha$ with $f_\alpha \in \bar{\mathcal{M}}_K(\Gamma(N), (k, \alpha))$.

Again, a p-adic modular quasiform of level 1 may be called a p-adic modular quasiform.

The ring of modular forms $\mathcal{M}(\Gamma)$ of course has a $\mathbf{Z}$-grading by weight. Similarly, the ring of reduced modular forms $\tilde{\mathcal{M}}(\Gamma)$ has a $\mathbf{Z}/(p-1)\mathbf{Z}$-grading if $p \neq 2, 3$, because by Theorem A, $\tilde{\mathcal{M}}(\Gamma) \simeq \bar{\mathbf{F}}_p[Q, R]/(\tilde{A} - 1)$, and $E_{p-1} = A(E_4, E_6)$ has weight $p-1$. To put it another way,

$$\tilde{\mathcal{M}}(\Gamma) = \bigoplus_{\alpha=1}^{p-1} \tilde{\mathcal{M}}^{\alpha}(\Gamma) \qquad \text{with} \quad \tilde{\mathcal{M}}^{\alpha}(\Gamma) = \sum_{k \equiv \alpha (p-1)} \tilde{\mathcal{M}}_{\bar{\mathbf{Q}}}(\Gamma, k).$$

Proposition 4 *If* $f = \sum_{\alpha=1}^{p-1} f_\alpha$ *is a* p*-adic modular quasiform,* $v_p(f) = \inf_\alpha v_p(f_\alpha)$.

Proof Observe that since $\mathcal{M}(\Gamma, k) = 0$ if $2 \nmid k$, only the f_α with α even can be nonzero. In particular, when $p = 2$ or 3, a p-adic modular quasiform is simply a p-adic modular form, and the proposition is trivial. Otherwise, let π be a uniformizing element of a field of definition K for f. Clearly $v_p(f) \geq \inf_\alpha v_p(f_\alpha)$. After multiplying f by an appropriate power of π, the proof of the reverse inequality amounts to showing that if each $v_p(f_\alpha) \geq 0$, and if $v_p(f) \geq lv_p(\pi)$ for a nonnegative integer l, then each $v_p(f_\alpha) \geq lv_p(\pi)$. This statement is trivially true if $l = 0$, so to prove it by induction on l, assume it is true for $l = m$. Since the $\tilde{\mathcal{M}}^{\alpha}(\Gamma)$ are linearly independent, one sees after approximating each f_α by a modular form that $v_p(f) \geq (m+1)v_p(\pi) > 0$ implies each $v_p(f_\alpha) > 0$. Hence $\pi^{-1}f = \sum_\alpha \pi^{-1}f_\alpha$ is a quasiform with $v_p(\pi^{-1}f) \geq mv_p(\pi)$ and $v_p(\pi^{-1}f_\alpha) \geq 0$, so by the inductive hypothesis $v_p(\pi^{-1}f_\alpha) \geq mv_p(\pi)$, i.e., $v_p(f_\alpha) \geq (m+1)v_p(\pi)$ for each α.

Corollary *The representation of a* p*-adic modular quasiform* f *as a sum* $\sum_{\alpha=1}^{p-1} f_\alpha$, $f_\alpha \in \tilde{\mathcal{M}}(\Gamma, (k, \alpha))$, *is unique.*

Proof It suffices to show that if $0 = \sum_\alpha f_\alpha$, then each $f_\alpha = 0$, and this is the special case $v_p(f) = \infty$ of the theorem.

Theorem A assures the validity for $\tilde{\mathcal{M}}_{\bar{\mathbf{Q}}}(\Gamma)$ of Serre's theory of filtration and the Θ-operator [9]. In particular, if $p \neq 2, 3$, the filtration of $\Theta^{p-2}(E_{p+1})$ is $p^2 - 1$. For the rest of this section, q denotes $e^{2\pi i z}$.

Proposition 5 *If* $k \in \mathbf{N}$ *and*

$$(p-1) \mid k, \qquad p \neq 2,$$
$$2 \mid k, \qquad p = 2,$$

then

$$\tilde{\phi} = \sum_{n=1}^{\infty} \tilde{\sigma}_{k-1}(n) q^n \notin \tilde{\mathcal{M}}(\Gamma).$$

Proof By elementary congruences $\tilde{\phi}^p - \tilde{\phi} = \tilde{\psi}$ where

$$\tilde{\psi} = \tfrac{1}{24}\Theta^{p-2}(\tilde{E}_{p+1})$$

if $p \neq 2, 3$ and $\tilde{\psi} = -\tilde{\Delta}$ if $p = 2$ or 3. The equation $\tilde{\phi}^p - \tilde{\phi} = -\tilde{\Delta}$ can clearly not be solved in $\tilde{\mathcal{M}}(\Gamma) = \bar{\mathbf{F}}_p(\tilde{\Delta})$, proving the proposition if $p = 2$ or 3. Otherwise, assume $\tilde{\phi} = \sum_\alpha \tilde{\phi}_\alpha$ with $\tilde{\phi}_\alpha \in \tilde{\mathcal{M}}^\alpha(\Gamma)$. As $p\alpha \equiv \alpha \bmod (p-1)$, $\tilde{\psi} = \tilde{\phi}^p - \tilde{\phi} = \sum_\alpha (\tilde{\phi}_\alpha^p - \tilde{\phi}_\alpha)$ with $\tilde{\phi}_\alpha^p - \tilde{\phi}_\alpha \in \tilde{\mathcal{M}}^\alpha(\Gamma)$. Since $\tilde{\psi}$ has filtration $p^2 - 1$, $\tilde{\phi}_\alpha^p - \tilde{\phi}_\alpha = 0$ for $\alpha \neq p-1$ and $\tilde{\phi}_\alpha^p - \tilde{\phi}_\alpha = \tilde{\psi}$ for $\alpha = p-1$. But if $\tilde{\phi}_{p-1}$ has any filtration h, $\tilde{\phi}_{p-1}^p$ and $\tilde{\phi}_{p-1}^p - \tilde{\phi}_{p-1}$ have filtration ph, which cannot equal $p^2 - 1$, a contradiction.

It is now possible to establish an analogue of Theorem B for p-adic modular quasiforms. The proof utilizes the Eisenstein–Serre series $E_k^* \in \bar{\mathcal{M}}_{\mathbf{Q}}(\Gamma, k)$ defined in [10], which have the property that $v_p(E^*_{(h,0)} - 1) = v_p(h) + 1$.

Theorem 6 *Suppose* $f^{(1)} = \sum_{\alpha=1}^{p-1} f_\alpha^{(1)}$ *and* $f^{(2)} = \sum_{\alpha=1}^{p-1} f_\alpha^{(2)}$ *are p-adic modular quasiforms of respective weights* k_1 *and* k_2, *with* $v_p(f^{(1)} - f^{(2)}) \geq v_p(f^{(1)}) + r$, $r > 0$. *Then* $v_p(k_1 - k_2) \geq r - 1$ *if* $p \neq 2$ *and* $v_p(k_1 - k_2) \geq r - 2$ *if* $p = 2$.

Proof Assume that K is a common field of definition for $f^{(1)}$ and $f^{(2)}$ with uniformizer π. If $p = 2$ or 3, $f^{(1)}$ and $f^{(2)}$ are actually p-adic modular forms so, by Theorem B, nothing remains to be done. If $p \neq 2, 3$, after multiplying $f^{(1)}$ and $f^{(2)}$ by an appropriate power of π, one may assume $v_p(f^{(1)}) = 0$, whence each $v_p(f_\alpha^{(1)})$, $v_p(f_\alpha^{(2)}) \geq 0$ by Proposition 4. If $k_2 > k_1$, let $h = k_2 - k_1$ and $m = v_p(h) + 1$, so the assertion is $m \geq r$. If this were not the case, i.e., $r > m$, then the inequalities $v_p(f^{(1)} - f^{(2)}) \geq r$ and $v_p(E^*_{(h,0)} - 1) \geq m$ applied to the equation $f^{(1)}E^*_{(h,0)} - f^{(2)} = (f^{(1)} - f^{(2)}) + f^{(1)}(E^*_{(h,0)} - 1)$ give first $v_p(f^{(1)}E^*_{(h,0)} - f^{(2)}) \geq m$ and then

$$p^{-m}(f^{(1)}E^*_{(h,0)} - f^{(2)}) \equiv p^{-m}f^{(1)}(E^*_{(h,0)} - 1) \bmod \pi. \tag{1}$$

Applying Proposition 4 to the p-adic modular quasiform $f^{(1)}E^*_{(h,0)} - f^{(2)}$ of weight k_2 yields $p^{-m}(f^{(1)}E^*_{(h,0)} - f^{(2)}) = \sum_\alpha g_\alpha$, $g_\alpha \in \tilde{\mathcal{M}}^\alpha(\Gamma)$, $v_p(g_\alpha) \geq 0$. The equation (1) may now be rewritten

$$\sum_\alpha g_\alpha = p^{-m}\left(\sum_\alpha f_\alpha^{(1)}\right)(E^*_{(h,0)} - 1) \bmod \pi. \tag{2}$$

Since the reduction of a p-adic modular form obviously equals the reduction of some modular form, and since

$$\tilde{\phi} = \widetilde{\lambda p^{-m}(E^*_{(h,0)} - 1)} \qquad \text{with} \quad v_p(\lambda) = 0,$$

(2) shows that $\tilde{\phi} = \lambda \sum_\alpha \tilde{g}_\alpha / \sum_\alpha \tilde{f}_\alpha$ is in the quotient field of $\tilde{\mathcal{M}}(\Gamma)$. But by Proposition 5 and its proof, $\tilde{\phi}^p - \tilde{\phi} = \tilde{\psi} \in \tilde{\mathcal{M}}(\Gamma)$ and $\tilde{\phi} \notin \tilde{\mathcal{M}}(\Gamma)$, while according to Section 1.2 of [10], $\tilde{\mathcal{M}}(\Gamma)$ is integrally closed. This contradiction to the assumption $m < r$ establishes the theorem.

Corollary 1 *If $f^{(1)} = \sum_\alpha f_\alpha^{(1)}$ and $f^{(2)} = \sum_\alpha f_\alpha^{(2)}$ are p-adic modular quasiforms and $m \in \mathbf{N}$, then $v_p(f^{(1)} - f^{(2)}) \geq m$ implies $v_p(f_\alpha^{(1)} - f_\alpha^{(2)}) \geq m$ for each α.*

Proof Again, the corollary is obvious if $p = 2$ or 3, and one may assume $v_p(f^{(1)}) = 0$ otherwise. If $f^{(1)}$ and $f^{(2)}$ have weights k_1 and k_2, then Theorem 6 gives $h = k_2 - k_1 \equiv 0 \bmod p^{m-1}$, so $f^{(1)}E^*_{(h,0)} - f^{(2)} \equiv f^{(1)} - f^{(2)} \equiv 0 \bmod p^m$. Since $f^{(1)}E^*_{(h,0)} - f^{(2)} = \sum_\alpha (f_\alpha^{(1)}E^*_{(h,0)} - f_\alpha^{(2)})$ is a p-adic modular quasiform of weight k_2, Proposition 4 now gives $f_\alpha^{(1)} - f_\alpha^{(2)} \equiv f_\alpha^{(1)}E^*_{(h,0)} - f_\alpha^{(2)} \equiv 0 \bmod p^m$.

Corollary 2 *The limit of a sequence of p-adic modular quasiforms $f^{(i)} = \sum_\alpha f_\alpha^{(i)}$ over K of weight k_i is a p-adic modular quasiform f over K of weight $k = \lim k_i$.*

Proof For each α, the $f_\alpha^{(i)}$ converge to some $f_\alpha \in K_p[[q]]$ by Corollary 1 and the completeness of K_p. Since each $f_\alpha \in \mathcal{M}_K(\Gamma, (k, \alpha))$, $f = \sum_\alpha f_\alpha$ is a p-adic modular quasiform of weight k.

Corollary 3 *If $f = \sum_{n=0}^\infty a_n q^n$ is a p-adic modular quasiform of weight k, then $v_p(a_0) \geq \inf_{n \geq 1} v_p(a_n) - v_p(k) - 1 - \delta_{2,p}$.*

Corollary 4 *Let $f^{(i)} = \sum_{n=0}^\infty a_n^{(i)} q^n$ be p-adic modular quasiforms over K of weight k_i, $i = 1, 2, \ldots$. Suppose that the $a_n^{(i)}$ tend uniformly toward some a_n for $n \geq 1$, and that the k_i approach a nonzero limit k in $\mathbf{Z}_p$. Then the $a_0^{(i)}$ have a limit a_0, and $f = \sum_{n=0}^\infty a_n q^n$ is a p-adic modular quasiform over K of weight k.*

Proof The proofs of Corollaries 3 and 4 are analogous to those of Corollaries C and D, with Theorem 6 replacing Theorem B.

We note that Theorem 6 can be deduced immediately from its Corollary 1. However, there is no obvious way of proving Corollary 1 directly. It does seem necessary to use the same methods Serre used to prove Theorem B once again.

3. Modular Forms on $\Gamma_{01}(p^r, N)$

Throughout this section, we fix a positive integer N, let p be a prime not dividing N, and write $(a, b : c, d)$ for the matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$. For each $r \in \mathbf{N}$, we

define three congruence subgroups of Γ by

$$\Gamma_0(p^r, N) = \{(a, b : c, d) \in \Gamma(N) \,|\, c \equiv 0 \bmod p^r\},$$
$$\Gamma_{01}(p^r, N) = \{(a, b : c, d) \in \Gamma(N) \,|\, c \equiv 0 \bmod p^r,\ a \equiv d \equiv 1 \bmod p\},$$
$$\Gamma_1(p^r, N) = \{(a, b : c, d) \in \Gamma(N) \,|\, c \equiv 0 \bmod p^r,\ a \equiv d \equiv 1 \bmod p^r\}.$$

We abbreviate $\Gamma_0(p^r) = \Gamma_0(p^r, 1)$, $\Gamma_{01}(p^r) = \Gamma_{01}(p^r, 1)$, and $\Gamma_1(p^r) = \Gamma_1(p^r, 1)$. There are isomorphisms $\Gamma_{01}(p^{r-1}, N)/\Gamma_{01}(p^r, N) \to \mathbf{Z}/p\mathbf{Z}$, $(a, b : p^{r-1}c, d) \mapsto c$, and $\Gamma_0(p^r, N)/\Gamma_{01}(p^r, N) \to (\mathbf{Z}/p\mathbf{Z})^\times$, $(a, b : c, d) \mapsto d$, where any integer is considered a member of $\mathbf{Z}/p\mathbf{Z}$ by the natural map. Since $\mathbf{Z}/p\mathbf{Z}$ and $(\mathbf{Z}/p\mathbf{Z})^\times$ are abelian, there are two incompatible decompositions of the space of modular forms on $\Gamma_{01}(p^r, N)$: one according to characters from $\Gamma_{01}(p^{r-1}, N)$, and the other according to characters from $\Gamma_0(p^r, N)$. Henceforward, ξ will always denote a character of $\mathbf{Z}/p\mathbf{Z}$, extendible to an additive character of $\mathbf{Z}$, and χ will denote a character of $(\mathbf{Z}/p\mathbf{Z})^\times$, extendible to a Dirichlet character of modulus p. Then

$$\mathscr{M}(\Gamma_{01}(p^r, N), k) = \bigoplus_{\xi \in (\mathbf{Z}/p\mathbf{Z})^*} \mathscr{M}(\Gamma_{01}(p^r, N), \xi, k) \qquad (r \geq 2)$$

$$\mathscr{M}(\Gamma_{01}(p^r, N), k) = \bigoplus_{\chi \in (\mathbf{Z}/p\mathbf{Z})^{\times *}} \mathscr{M}(\Gamma_{01}(p^r, N), \chi, k) \qquad (r \geq 1).$$

Here $\mathscr{M}(\Gamma_{01}(p^r, N), \xi, k) = \{f \in \mathscr{M}(\Gamma_{01}(p^r, N), k) \text{ s.t. } f|_k(a, b : p^{r-1}c, d) = \xi(c)f \text{ for } (a, b : p^{r-1}c, d) \in \Gamma_{01}(p^{r-1}, N)\}$ and $\mathscr{M}(\Gamma_{01}(p^r, N), \chi, k) = \{f \in \mathscr{M}(\Gamma_{01}(p^r, N), k) \text{ s.t. } f|_k(a, b : c, d) = \chi(d)f \text{ for } (a, b : c, d) \in \Gamma_0(p^r, N)\}$. Analogous decompositions of course hold for $\mathscr{M}(\Gamma_1(p^r, N), k)$.

The goal of this section is to prove that a modular form of level N on $\Gamma_0(p^r)$ is a p-adic modular form of the same level and weight, i.e., $\mathscr{M}(\Gamma_0(p^r, N), k) \subset \bar{\mathscr{M}}(\Gamma(N), (k, k))$. A reasonable strategy for doing this would be first to prove it directly for forms on $\Gamma_0(p, N)$ and certain Eisenstein series on $\Gamma_0(p^r, N)$ having characters with respect to $\Gamma_0(p^{r-1}, N)$. The Eisenstein series could then be used to inductively reduce the theorem from $\Gamma_0(p^r, N)$ to $\Gamma_0(p, N)$. However, since $\Gamma_0(p^r, N)$ is not a normal subgroup of $\Gamma_0(p^{r-1}, N)$, the desired characters do not exist. So instead we apply the strategy to show inductively that forms on $\Gamma_{01}(p^r, N)$, which *is* a normal subgroup of $\Gamma_{01}(p^{r-1}, N)$, are p-adic modular quasiforms of level N. The decomposition of $\mathscr{M}(\Gamma_{01}(p^r, N), k)$ with respect to characters from $\Gamma_0(p^r, N)$ may then be employed to prove the desired result.

Proposition 7 *Any modular form on $\Gamma_0(p, N)$ of weight k is a p-adic modular form of level N and weight (k, k), i.e., $\mathscr{M}_K(\Gamma_0(p, N), k) \subset \bar{\mathscr{M}}_K(\Gamma(N), (k, k))$.*

Proof Choose integers α and γ such that $\alpha p - \gamma N^2 = 1$, let $m = pN$, and write $W = (p\alpha, N : m\gamma, p)$ so $\det W = p$. Set $A = (p, 0 : 0, 1)$, $S^j = (1, Nj : 0, 1)$, $T = (p\alpha, N : N\gamma, 1)$,

$$\Gamma^0(p, N) = \{(a, b : c, d) \in \Gamma(N) \mid b \equiv 0 \bmod p\}.$$

Write $f \mid$ for $f \mid_{wt\, f}$ and $f \mid U^*$ for $\sum_{j=1}^{p} f \mid A^{-1} \mid S^j$, so $f \mid U^* = p^{1 - wt\, f/2} f \mid U$. We claim that if $f \in \mathcal{M}(\Gamma_0(p, N), k)$, then $(f \mid W + f \mid U^*) \in \mathcal{M}(\Gamma(N), k)$. First, $f \mid A^{-1} \in \mathcal{M}(\Gamma^0(p, N), k)$ because

$$(1/p, 0 : 0, 1)(x, py : z, w)(p, 0 : 0, 1) = (x, y : pz, w).$$

Second, the $p + 1$ matrices T, S^j $(1 \leq j \leq p)$ form a complete set of right coset representatives of $\Gamma^0(p, N)$ in $\Gamma(N)$. Indeed, a trivial calculation shows that they lie in different cosets, while the set $\Gamma(N)/\Gamma^0(p, N)$ injects into $\Gamma/\Gamma^0(p)$, which has $p + 1$ elements. Putting these facts together,

$$f \mid W + f \mid U^* = (f \mid A^{-1}) \mid T + \sum_{j=1}^{p} (f \mid A^{-1}) S^j \in \mathcal{M}(\Gamma(N), k),$$

as desired. Moreover, another simple calculation shows that W normalizes $\Gamma_0(p, N)$, so that if $f \in \mathcal{M}(\Gamma_0(p, N), k)$, then $f \mid W^{-1} \in \mathcal{M}(\Gamma_0(p, N), k)$ and $(f + f \mid W^{-1} \mid U^*) \in \mathcal{M}(\Gamma(N), k)$.

For a fixed even integer $l \geq 4$ with $(p - 1) \mid l$, let $E = E_l$ and $g = E - p^{l/2} E \mid W \in \mathcal{M}(\Gamma_0(p, N), k)$. Then $g \equiv 1 \bmod p$ and $g \mid W^{-1} \equiv 0 \bmod p^{1 + l/2}$. In fact,

$$\begin{aligned} E \mid W &= E \mid (p\alpha, N : m\gamma, p) = E \mid (\alpha, N : N\gamma, p)(p, 0 : 0, 1) \\ &= E \mid (p, 0 : 0, 1) = p^{l/2} E \mid V \end{aligned}$$

since $(\alpha, N : N\gamma, p) \in \Gamma$, and similarly $E \mid W^{-1} = p^{l/2} E \mid V$. Because $E \equiv 1 \bmod p$, $g = E - p^l E \mid V \equiv 1 \bmod p$, and

$$\begin{aligned} g \mid W^{-1} &= (E - p^{l/2} E \mid W) \mid W^{-1} = E \mid W^{-1} - p^{l/2} E \\ &= p^{l/2} (E \mid V - E) \equiv 0 \bmod p^{1 + l/2}. \end{aligned}$$

Finally, if $f \in \mathcal{M}(\Gamma_0(p, N), k)$, define $f_m = f g^{p^m} + f g^{p^m} \mid W^{-1} \mid U^*$ for each $m \in \mathbf{N}$. Since $f g^{p^m}$ is on $\Gamma_0(p, N)$, f_m is on $\Gamma(N)$ by the remarks above. To prove the theorem, one needs $f_m \to f$ as $m \to \infty$. Write $k_m = k + lp^m$ so $f_m = f g^{p^m} + p^{1 - k_m/2} (f g^{p^m}) \mid W^{-1} \mid U$. $f g^{p^m} \to f$ because $g \equiv 1 \bmod p$, and it remains to show $(p^{1 - k_m/2}) f g^{p^m} \mid W^{-1} \mid U \to 0$. Indeed,

$$\begin{aligned} v_p(p^{1 - k_m/2} f g^{p^m} \mid W^{-1} \mid U) &\geq v_p((p^{1 - k_m/2}) f g^{p^m} \mid W^{-1}) \\ &= v_p(f \mid W^{-1}) + p^m v_p(g \mid W^{-1}) + 1 - k_m/2 \\ &\geq v_p(f \mid W^{-1}) + 1 - k/2 + p^m \to \infty. \end{aligned}$$

From now on, let ω denote the unique character of $(\mathbf{Z}/p\mathbf{Z})^\times$ such that $v_p(\omega(x) - x) > 0$ for all $x \in \mathbf{Z}$. Clearly ω generates the character group $(\mathbf{Z}/p\mathbf{Z})^{\times *}$, that is, $\omega^1, \omega^2, \ldots, \omega^{p-1}$ is a complete list of characters of $(\mathbf{Z}/p\mathbf{Z})^\times$. We always consider each ω^j to be a Dirichlet character *of modulus* p, so in particular $\omega^{p-1}(n) = 0$ if $p \mid n$, and the L-series $L(s, \omega^{p-1}) = (1 - p^{-s})\zeta(s)$. In the future, when discussing modular forms on Γ or $\Gamma_{01}(p^r)$, q will denote $e^{2\pi iz}$. But when these forms are used in conjunction with forms for $\Gamma(N)$, they should be viewed as series in q^N with $q = e^{2\pi iz/N}$.

Proposition 8 *Any modular form on $\Gamma_{01}(p, N)$ of character ω^γ and weight k is a p-adic modular form of level N and weight $(k, k + \gamma)$, i.e., $\mathscr{M}_K(\Gamma_{01}(p, N), \omega^\gamma, k) \subset \bar{\mathscr{M}}_K(\Gamma(N), (k, k + \gamma))$.*

Proof First note that the series

$$G_k(\omega^j) = G_k(q, \omega^j) = L(1 - k, \omega^j) + \sum_{n=1}^{\infty} \sum_{v \mid n} (\operatorname{sgn} v)\omega^j(v)v^{k-1}q^n$$

lies in $\mathscr{M}(\Gamma_{01}(p), \omega^j, k)$, as shown by its expression as a sum of Eisenstein series of level p. It follows directly from Theorem 3 of [1] (see Lemma 13 of this paper) that if $(p - 1) \mid (k + \gamma)$ and $p \neq 2$, then $v_p(L(1 - k, \omega^j) = v_p(B^k_{\omega^j}/k) = -1 - v_p(k)$. Hence, in that case

$$E_k(\omega^j) = L(1 - k, \omega^j)^{-1}G_k(\omega^j) \equiv 1 \bmod p^{v_p(k)+1}.$$

If $p = 2$, $\mathscr{M}_K(\Gamma_{01}(p, N), \omega^\gamma, k) = \mathscr{M}_K(\Gamma_0(p, N), k) \subset \bar{\mathscr{M}}_K(\Gamma(N), (k, k)) = \bar{\mathscr{M}}_K(\Gamma(N), (k, k + \gamma))$ by Proposition 7. If $p \neq 2$, suppose $f \in \mathscr{M}_K(\Gamma_{01}(p, N), \omega^\gamma, k)$ and let $k_m = p^m(p - 1) + \gamma$. Then

$$f = \lim_{m \to \infty} fE_{k_m}(\bar{\omega}^\gamma)$$

while

$$fE_{k_m}(\bar{\omega}^\gamma) \in \mathscr{M}_{K(\zeta_{p^{-1}})}(\Gamma_{01}(p, N), \omega^\gamma\bar{\omega}^\gamma, k + k_m) = \mathscr{M}_{K(\zeta_{p^{-1}})}(\Gamma_0(p, N), k + k_m).$$

Thus, f is a p-adic modular form of level N and weight $k + \gamma = \lim_{m \to \infty} (k + k_m)$ by Proposition 7. That f is in fact defined over K as a p-adic modular form of level N follows from Corollary 2.1.

We now commence the second part of our strategy by considering certain Eisenstein series. In all that follows, summations such as $\sum_{v \mid n}$ and $\sum_{v \equiv n}$ will be over both negative and positive integers v excluding 0.

Proposition 9 *For any integer $k > 2$ and any character ξ of $\mathbf{Z}/p\mathbf{Z}$,*

$$H_k(\xi) = \alpha_k(p) + \sum_{n=1}^{\infty} \sum_{v \mid n} \xi(-n/v)(\operatorname{sgn} v)v^{k-1}q^n \in \mathscr{M}(\Gamma_{01}(p^2), \xi, k),$$

where $\alpha_k(p) = \lambda_k(p) \sum_{n \equiv 1 (p)} n^{-k}$ *and* $\lambda_k(p) = p^k(k-1)!/(-2\pi i)^k$. *Also* $\alpha_k(p) \in \mathbf{Q}(\zeta_p)$ *and if*

$$(p-1) \mid k, \qquad p \neq 2$$
$$2 \mid k, \qquad p = 2,$$

then $v_p(\alpha_k(p)) = -1 - v_p(k)$.

Proof The Eisenstein series of level p,

$$G_k(\tau, c, d, p) = \alpha_k(c, d, p) + \sum_{n=1}^{\infty} \sum_{\substack{v \mid n \\ n/v \equiv c (p)}} (\operatorname{sgn} v) v^{k-1} \zeta_p^{dv} \tau^n$$

are modular forms on $\Gamma(p)$ [8]. Here $\tau = e^{2\pi i z/p}$, $\zeta_p = e^{2\pi i/p}$, $\alpha_k(c, d, p) = 0$ if $c \not\equiv 0 \bmod p$, and $\alpha_k(c, d, p) = \lambda_k(p) \sum_{n \equiv d (p)} n^{-k}$ if $c \equiv 0 \bmod p$. Furthermore. $G_k(\tau, c, d, p) \mid L = G_k(\tau, (c, d)L, p)$ for $L \in \Gamma$, and $G_k(q, c, d, p) = p^{-k/2} G_k(\tau, c, d, p) \mid (p, 0 : 0, 1)$. Hence, $G_k(q, c, d, p) \mid x, y : pz, w) = G_k(q, cx + dz, dw, p)$ if $(x, y : pz, w) \in \Gamma_0(p)$. In particular, if $d = 1$ and $(x, y : pz, w) \in \Gamma_{01}(p)$, then $G_k(q, c, 1, p) \mid (x, y : pz, w) = G_k(q, c + z, 1, p)$. Therefore

$$\sum_{c=1}^{p} \xi(-c) G_k(q, c, 1, p) \mid (x, y : pz, w) = \xi(z) \sum_{c=1}^{p} \xi(-c) G_k(q, c, 1, p),$$

i.e., $\sum_{i=1}^{p} \xi(-c) G_k(q, c, 1, p) \in \mathcal{M}(\Gamma_{01}(p^2), \xi, k)$. The first assertion of the theorem now follows upon observing that in fact

$$H_k(\xi) = H_k(q, \xi) = \sum_{c=1}^{p} \xi(-c) G_k(q, c, 1, p).$$

To show $\alpha_k(p) \in \mathbf{Q}(\zeta_p)$, let σ be an automorphism of $\mathbf{C}$ over $\mathbf{Q}(\zeta_p)$. Since $H_k(\xi) \in \mathcal{M}(\Gamma_1(p^2), k)$ and $\mathcal{M}(\Gamma_1(p^2), k)$ has a basis over $\mathbf{Q}$, $H_k(\xi)^\sigma \in \mathcal{M}(\Gamma_1(p^2), k)$. Thus $H_k(\xi) - H_k(\xi)^\sigma$ is a modular form on $\Gamma_1(p^2)$ of weight k. But since all coefficients of $H_k(\xi)$ except possibly the first lie in $\mathbf{Q}(\zeta_p)$, $H_k(\xi) - H_k(\xi)^\sigma = \alpha_k(p) - \alpha_k(p)^\sigma$, a modular form on $\Gamma_1(p^2)$ of weight 0. This is impossible unless $\alpha_k(p)^\sigma = \alpha_k(p)$.

It remains to evaluate $v_p(\lambda_k(p) \sum_{n \equiv 1 (p)} n^{-k})$ when

$$(p-1) \mid k, \qquad p \neq 2$$
$$2 \mid k, \qquad p = 2.$$

If $p = 2$,

$$\sum_{n \equiv 1 (p)} n^{-k} = 2(1 - 2^{-k})\zeta(k)$$

and

$$v_p(\lambda_k(p)\sum_{n\equiv 1\ (p)} n^{-k}) = v_p((2^k-1)B_k/k) = -1 - v_p(k).$$

If $p \neq 2$,

$$\sum_{n\equiv 1\ (p)} n^{-k} = \sum_{\substack{n=1\\ n\equiv \pm 1\ (p)}}^{\infty} n^{-k} = (2/(p-1))\sum_{n=1}^{\infty} \sum_{1\le j\le p-1}^{j\ \text{even}} \omega^j(n)n^{-k}$$

$$= (2/(p-1))\sum_{1\le j\le p-1}^{j\ \text{even}} L(k, \omega^j)$$

since $\omega^2, \omega^4, \ldots, \omega^{p-1}$ is a complete list of characters of $(\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$ and k is even. Now, on the one hand $L(k, \omega^{p-1}) = (1-p^{-k})\zeta(k)$ so $v_p(\lambda_k(p)L(k, \omega^{p-1})) = v_p((p^k-1)B_k/2k) = -1 - v_p(k)$. On the other hand, if $j \neq p-1$, there is a functional equation $\lambda_k(p)L(k, \omega^j) = \tau(\omega^j)L(1-k, \bar{\omega}^j)$ with $\tau(\omega^j) = \sum_{x=1}^{p-1} \omega^j(x)\zeta_p^x$ a Gauss sum. Since

$$G_k(\bar{\omega}^j) = L(1-k, \bar{\omega}^j)$$

$$+ \sum_{n=1}^{\infty}\sum_{v|n} \bar{\omega}^j(v)(\operatorname{sgn} v)v^{k-1}q^n \in \mathcal{M}(\Gamma_{01}(p), \bar{\omega}^j, k)$$

$$\subset \bar{\mathcal{M}}(\Gamma, k-j)$$

by Proposition 8, Corollary C gives $v_p(L(1-k, \bar{\omega}^\gamma) \geq 0$. Putting these facts together,

$$v_p(\lambda_k(p)\sum_{n\equiv 1\ (p)} n^{-k}) = v_p(L(k, \omega^{p-1})\lambda_k(p) + \sum_{1\le j<p-1}^{j\ \text{even}} \lambda_k(p)L(k, \omega^j))$$

$$= -1 - v_p(k).$$

We shall now show that $H_k(\xi) \in \mathcal{M}(\Gamma_{01}(p^2), k)$ is a p-adic modular quasiform in a way that is consistent with the decomposition $\mathcal{M}(\Gamma_{01}(p^2), k) = \oplus_\chi \mathcal{M}(\Gamma_{01}(p^2), \chi, k)$.

Proposition 10 *Let $k > 2$, $\xi \in (\mathbf{Z}/p\mathbf{Z})^*$ and $H_k(\xi) = \sum_{\gamma=1}^{p-1} H_k^\gamma(\xi)$ with $H_k^\gamma(\xi) \in \mathcal{M}(\Gamma_{01}(p^2), \omega^\gamma, k)$. Then $H_k^\gamma(\xi) \in \mathcal{M}(\Gamma, (k, k+\gamma))$.*

Proof For any $f \in \mathcal{M}(\Gamma_{01}(p^2), k)$, the ω^γ-component of f is $f^\gamma = (1/(p-1))\sum_{x=1}^{p-1} \bar{\omega}^\gamma(x) f\,|R_x$ where $R_x \in \Gamma$,

$$R_x \equiv (x^{-1}, 0 : 0, x) \bmod p^2.$$

In particular,

$$(p-1)H_k^\gamma(\xi) = \sum_{x=1}^{p-1} \bar{\omega}^\gamma(x)\sum_{c=1}^{p-1} \xi(-c)G_k(q, c, 1, p)\,|R_x,$$

or after writing $\xi(1) = \xi_p^m$ and performing a short calculation:

$$(p-1)H_k^\gamma(\xi) = \lambda_k(p) \sum_n \bar{\omega}^\gamma(n) n^{-k} + \sum_{n=1}^{\infty} \sum_{v|n} \sum_{x=1}^{p-1} \bar{\omega}^\gamma(x) \zeta_p^{(v-mn/v)x} (\operatorname{sgn} v) v^{k-1} q^n \tag{3}$$

This series will be shown to be a p-adic modular form of weight $(k, k+\gamma)$ by expressing it as a sum of the known p-adic modular forms discussed below.

We have seen that

$$G_k(\omega^i) = L(1-k, \omega^i) + \sum_{n=1}^{\infty} \sum_{v|n} \omega^i(v) (\operatorname{sgn} v) v^{k-1} q^n$$

is a p-adic modular form of weight $(k, k+i)$ by Proposition 8. Note that if k and i do not have the same parity, $G_k(\omega^i)$ is identically zero. If R_h is Serre's differential operator,

$$\begin{aligned} G_k(\omega^i, \omega^j) &= G_k(q, \omega^i, \omega^j) \\ &= G_k(q, \omega^i) \mid R_{(0,j)} \\ &= \sum_{n=1}^{\infty} \sum_{v|n} \omega^i(v) \omega^j(n) (\operatorname{sgn} v) v^{k-1} q^n \end{aligned}$$

is a p-adic modular form of weight $(k, k+i+2j)$. Finally, if $1 \le c, d \le p-1$,

$$\begin{aligned} G_k(c, d) &= G_k(q, c, d) \\ &= \sum_{\substack{n=1 \\ n \equiv d}}^{\infty} \sum_{\substack{v|n \\ v \equiv c \,(p)}} (\operatorname{sgn} v) v^{k-1} q^n \\ &= (p-1)^{-2} \sum_{i=1}^{p-1} \sum_{j=1}^{p-1} \bar{\omega}^i(c) \bar{\omega}^j(d) G_k(q, \omega^i, \omega^j) \end{aligned}$$

is a p-adic modular quasiform of weight k.

First, suppose that $\gamma \neq p-1$. Then $\sum_{x=1}^{p-1} \bar{\omega}^\gamma(x) \zeta_p^{(v-mn/v)x} = 0$ if $v - mn/v \equiv 0 \bmod p$, and

$$\sum_{x=1}^{p-1} \bar{\omega}^\gamma(x) \zeta_p^{(v-mn/v)x} = \omega^\gamma(v - mn/v) \tau(\bar{\omega}^\gamma)$$

if $v - mn/v \not\equiv 0$. Applying this fact and the functional equation of $L(k, \bar{\omega}^\gamma)$ to (3) gives

$$(p-1)\tau(\bar{\omega}^\gamma)^{-1} H_k^\gamma(\xi) = L(1-k, \omega^\gamma) + \sum_{n=1}^{\infty} \sum_{v|n} \omega^\gamma(v - mn/v) (\operatorname{sgn} v) v^{k-1} q^n.$$

This expression can be written as the sum of three series, each of which is a

p-adic modular form of weight $(k, k+\gamma)$. Indeed,

$$(p-1)\tau(\bar{\omega}^{\gamma})^{-1}H_k^{\gamma}(\xi) = \left[L(1-k,\omega^{\gamma}) + \sum_{\substack{n=1\\ p|n}}^{\infty}\sum_{\substack{v|n\\ p\nmid v}} T(v,n)q^n\right] + \left[\sum_{\substack{n=1\\ p\nmid n}}^{\infty}\sum_{v|n} T(v,n)q^n\right] + \left[\sum_{\substack{n=1\\ p|n}}^{\infty}\sum_{\substack{v|n\\ p|v}}^{\infty} T(v,n)q^n\right]$$

where $T(v,n) = \omega^{\gamma}(v - mn/v)(\operatorname{sgn} v)v^{k-1}$. The first term is

$$L(1-k,\omega^{\gamma}) + \sum_{p|n}\sum_{v|n}\omega^{\gamma}(v)(\operatorname{sgn} v)v^{k-1}q^n = H_k(\omega^{\gamma})\,|\,U\,|\,V,$$

a p-adic modular form of weight $(k, k+\gamma)$.

The second term is

$$\sum_{c,d=1}^{p-1}\omega^{\gamma}(c-md/c)G_k(c,d) = \sum_{c,d=1}^{p-1}\omega^{\gamma}(c-md/c)\sum_{i,j=1}^{p-1}\bar{\omega}^i(c)\bar{\omega}^j(d)G_k(\omega^i,\omega^j).$$

The coefficient of a particular $G_k(\omega^i,\omega^j)$ in this expression is

$$\begin{aligned}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}&\omega^{\gamma}(c-md/c)\bar{\omega}^i(c)\bar{\omega}^j(d)\\ &= \sum_{c=1}^{p-1}\sum_{d=1}^{p-1}\omega^{\gamma}(c-mc^2d/c)\bar{\omega}^i(c)\bar{\omega}^j(c^2d)\\ &= \sum_{c=1}^{p-1}\omega^{\gamma-i-2j}(c)\sum_{d=1}^{p-1}\omega^{\gamma}(1-md)\bar{\omega}^j(d),\end{aligned}$$

and this is zero unless $i + 2j \equiv \gamma \bmod (p-1)$. Hence, the second term is a linear combination of those $G_k(\omega^i,\omega^j)$ with weight $(k, k+\gamma)$.

The third term is

$$\begin{aligned}&\omega^{\gamma}(-m)\sum_{\substack{n=1\\ p|n}}^{\infty}\sum_{\substack{v|n\\ p|v}}\omega^{\gamma}(n/v)(\operatorname{sgn} v)v^{k-1}q^n\\ &\quad= \omega^{\gamma}(-m)\sum_{t=1}^{\infty}\sum_{\substack{n=1\\ p|n}}^{\infty}\sum_{\substack{v|n\\ v_p(v)=t}}\omega^{\gamma}(n/v)(\operatorname{sgn} v)v^{k-1}q^n\\ &\quad= \omega^{\gamma}(-m)\sum_{t=1}^{\infty}(p^{t(k-1)})\left(\sum_{n=1}^{\infty}\sum_{v|n}\omega^{\gamma}(n)\bar{\omega}^{\gamma}(v)(\operatorname{sgn} v)v^{k-1}q^n\right)\Bigg|\,V^t\\ &\quad= \omega^{\gamma}(-m)\sum_{v=1}^{\infty}p^{t(k-1)}G_k(\bar{\omega}^{\gamma},\omega^{\gamma})\,|\,V^t.\end{aligned}$$

Since $G_k(\bar{\omega}^\gamma, \omega^\gamma)$ is a p-adic modular form of weight $(k, k-\gamma+2\gamma) = (k, k+\gamma)$, so is the third term.

Now suppose $\gamma = p-1$. Then $\sum_{x=1}^{p-1} \bar{\omega}^\gamma(x)\zeta_p^{(v-mn/v)x} = p-1$ or -1 as $(v - mn/v) \equiv 0$ or $\not\equiv 0 \bmod p$. It follows easily that

$$(p-1)H_k^\gamma(\xi) = -\left[\lambda_k(p)p^{-k}\sum_n n^{-k} + \sum_{n=1}^{\infty}\sum_{v|n}(\operatorname{sgn} v)v^{k-1}q^n\right]$$
$$+ p\left[\sum_{\substack{n=1\\ p\nmid n}}^{\infty}\sum_{\substack{v|n\\ v-mn/v\equiv 0}}(\operatorname{sgn} v)v^{k-1}q^n\right] + p\left[\lambda_k(p)p^{-1}\sum_n n^{-k}\right.$$
$$\left. + \sum_{n=1}^{\infty}\sum_{\substack{v|n,\ p|v\\ v-mn/v\equiv 0}}(\operatorname{sgn} v)v^{k-1}q^n\right].$$

The first term is zero if k is odd and an ordinary Eisenstein series if k is even—certainly a p-adic modular form of weight (k, k). The second term is

$$p\sum_{c=1}^{p-1}\sum_{\substack{d=1\\ c-md/c\equiv 0}}^{p-1} G_k(c, d) = p(p-1)^{-2}\sum_{c=1}^{p-1}\sum_{\substack{d=1\\ c-md/c\equiv 0}}^{p-1}\sum_{i,j=1}^{p-1}\bar{\omega}^i(c)\bar{\omega}^j(d)G_k(\omega^i, \omega^j),$$

in which sum the only $G_k(\omega^i, \omega^j)$ having nonzero coefficients are such that $i + 2j \equiv 0 \equiv \gamma \bmod(p-1)$. Finally, the third term equals

$$p\sum_{t=1}^{\infty}(p^{t(k-1)})\left[\lambda_k(p)p^{-k}(1-p^{k-1})\sum_n n^{-k} + \sum_{n=1}^{\infty}\sum_{\substack{v|n\\ p\nmid v}}(\operatorname{sgn} v)v^{k-1}q^n\right]\Big| V^t$$
$$= p\sum_{t=1}^{\infty} p^{t(k-1)}G_k(\omega^{p-1})\,|\,V^t \in \mathcal{M}(\Gamma, k) = \mathcal{M}(\Gamma, (k, k+\gamma)),$$

completing the proof.

For any character ξ and even integer $k > 2$, let $E_k(\xi) = \alpha_k(p)^{-1}H_k(\xi)$. Then $E_{-k}(\xi) = 1/E_k(\xi)$ is a meromorphic modular form on $\Gamma_{01}(p^2)$ of weight $-k$. Moreover, $E_{-k}(\xi) = \sum_{\gamma=1}^{p-1} E_{-k}^\gamma(\xi)$ with

$$E_{-k}^\gamma(\xi) = (p-1)^{-1}\sum_{x=1}^{p-1}\bar{\omega}^\gamma(x)E_{-k}(\xi)\,|\,R_x$$

a meromorphic modular form on $\Gamma_{01}(p^2)$ of character ω^γ and weight $-k$. Each $E_{-k}^\gamma(\xi)$ has a finite-tailed Laurent expansion in q, valid in some neighborhood of $i\infty$.

Proposition 11 *Let ξ be a character of $\mathbf{Z}/p\mathbf{Z}$ and let $k > 2$ be an integer such that*

$$(p-1)\,|\,k, \qquad p \neq 2,$$
$$2\,|\,k, \qquad p = 2.$$

Then the q-expansion of each $E^{\gamma}_{-k}(\xi)$ *lies in* $\bar{\mathbf{Q}}[[q]]$ *and is a p-adic modular form of weight* $(-k, -k+\gamma)$.

Proof Write E_k for $E_k(\xi)$, so $E_k = 1 + p\sum_{n=1}^{\infty} a_n q^n$ with $a_n \in \mathbf{Q}(\zeta_p)$ and $v_p(a_n) \geq 0$, by Proposition 9. Therefore, $E_k^{p^m-1}$ approaches a limit in $\Omega_p[[q]]$ as $m \to \infty$, and that limit is $E_{-k} = 1/E_k$. But by Proposition 10, E and thus E^{p^m-1} are p-adic modular quasiforms. Corollary 2 of Theorem 6 hence implies that E_{-k} is a p-adic modular quasiform of weight $-k$, i.e., $E_{-k} = \sum \hat{E}^{\gamma}_{-k}$ with $\hat{E}^{\gamma}_{-k} \in \bar{\mathcal{M}}(\Gamma, (-k, -k+\gamma))$. On the other hand, we already know that $E_{-k} = \sum E^{\gamma}_{-k}$ with E^{γ}_{-k} a Laurent series representing a meromorphic modular form on $\Gamma_{01}(p^2)$ of character ω^{γ} and weight $-k$.

By Proposition 10, E_k itself equals $\sum E_k^{\gamma}$ with $E_k^{\gamma} \in \bar{\mathbf{Q}}[[q]]$ both a modular form on $\Gamma_{01}(p^2)$ of character ω^{γ} and weight k, *and* a p-adic modular form of weight $(k, k+\gamma)$. The fact that $(\sum_{\gamma_1=1}^{p-1} E_k^{\gamma_1})(\sum_{\gamma_2=1}^{p-1} \hat{E}^{\gamma_2}_{-k}) = 1$ is equivalent, by the corollary to Proposition 4, to a system of $p-1$ linear equations in the $p-1$ "variables" $\hat{E}^{\gamma_2}_{-k}$, namely

$$\sum_{\gamma_1+\gamma_2 \equiv \beta\,(p-1)} E_k^{\gamma_1}\hat{E}^{\gamma_2}_{-k} = \delta_{\beta,\,p-1} \qquad (1 \leq \beta \leq p-1).$$

And the fact that $(\sum_{\gamma_1=1}^{p-1} E_k^{\gamma_1})(\sum_{\gamma_2=1}^{p-1} E_k^{\gamma_2}) = 1$ is equivalent, by linear independence of forms with different characters, to the same system of linear equations in the variables $E^{\gamma_2}_{-k}$, namely

$$\sum_{\gamma_1+\gamma_2 \equiv \beta\,(p-1)} E_k^{\gamma_1}E^{\gamma_2}_{-k} = \delta_{\beta,\,p-1} \qquad (1 \leq \beta \leq p-1).$$

Since the theorem will be proved if $E^{\gamma}_{-k} = \hat{E}^{\gamma}_{-k}$, it suffices to show that the constant term of the series represented by the determinant of the system of linear equations is not zero. The determinant is clearly a cyclic determinant with first row $(\beta = 1)$ $(E_k^{p-1}, E_k^{p-2}, \ldots, E^1)$. By Eq. (3), the constant term of E_k^{γ} is $\lambda_k(p)\sum_n \bar{\omega}^{\gamma}(n)n^{-k}/(p-1)\alpha_k(p)$. Hence, up to a nonzero factor, the constant term of the determinant is given by a cyclic determinant with first row $(\sum_n \bar{\omega}^{p-1}(n)n^{-k}, \ldots, \sum_n \bar{\omega}^1(n)n^{-k})$. The value of a cyclic determinant with first row $(a_1, a_2, \ldots, a_m)$ is $\prod_{i=1}^{m}(\sum_{j=1}^{m} a_j\zeta_m^{ij})$ [7], or in the present case

$$\prod_{i=1}^{p-1}\left(\sum_{j=1}^{p-1}\sum_{n}\bar{\omega}^j(n)n^{-k}\zeta_{p-1}^{ij}\right) = (p-1)^{p-1}\prod_{x=1}^{p-1}\left(\sum_{n\equiv x\,(p)} n^{-k}\right) \neq 0.$$

We are now ready to prove the main theorem of this section.

Theorem 12 *Any modular form on* $\Gamma_{01}(p^r, N)$ *of character* ω^{γ} *and weight* k *is a p-adic modular form of level* N *and weight* $(k, k+\gamma)$, *that is,* $\mathcal{M}_K(\Gamma_{01}(p^r, N), \omega^{\gamma}, k) \subset \bar{\mathcal{M}}_K(\Gamma(N), (k, k+\gamma))$.

Proof By Corollary 2.1, it is only necessary to show $\mathcal{M}(\Gamma_{01}(p^r, N), \omega^{\gamma}, k) \subset \bar{\mathcal{M}}(\Gamma(N), (k, k+\gamma))$. In fact we shall prove by induc-

tion on r the equivalent statement $S(r)$: If $f \in \mathcal{M}(\Gamma_{01}(p^r, N), k)$ and $f = \sum_{\gamma=1}^{p-1} f^\gamma$ with $f^\gamma \in \mathcal{M}(\Gamma_{01}(p^r, N), \omega^\gamma, k)$, then each

$$f^\gamma \in \bar{\mathcal{M}}(\Gamma(N), (k, k+\gamma)).$$

For $r = 1$, this is Proposition 8.

It follows from a trivial matrix computation that if $g(q) \in \mathcal{M}(\Gamma_{01}(p^r), \xi, k)$, then $g(q^p) = g(q) \mid V \in \mathcal{M}(\Gamma_{01}(p^{r+1}), \xi, k)$; and if $g(q) \in \mathcal{M}(\Gamma_{01}(p^r), \omega^\gamma, k)$, then $g(q) \mid V \in \mathcal{M}(\Gamma_{01}(p^{r+1}), \omega^\gamma, k)$. Consequently, $E_k(q^{p^r}, \xi) \in \mathcal{M}(\Gamma_{01}(p^{r+2}), \xi, k)$ and $E_k^\gamma(q^{p^r}, \xi) \in \mathcal{M}(\Gamma_{01}(p^{r+2}), \omega^\gamma, k)$. Similarly, $E_{-k}(q^{p^r}, \xi) \in \mathcal{A}(\Gamma_{01}(p^{r+2}), \xi, k)$ and

$$E_{-k}^\gamma(q^{p^r}, \xi) \in \mathcal{A}(\Gamma_{01}(p^{r+2}), \omega^\gamma, k)$$

where $\mathcal{A}$ refers to meromorphic modular forms. And of course $E_k^\gamma(q^{p^r}, \xi)$ and $E_{-k}^\gamma(q^{p^r}, \xi)$ are still p-adic modular forms of respective weights $(k, k+\gamma)$ and $(-k, -k+\gamma)$.

Another simple observation is needed. Suppose that $f_1 \in \mathcal{M}(\Gamma_{01}(p^{r+1}, N), k_1)$, $f_2 \in \mathcal{A}(\Gamma_{01}(p^{r+1}, N), k_2)$,

$$f_3 = f_1 f_2 \in \mathcal{M}(\Gamma_{01}(p^{r+1}, N), k_1 + k_2).$$

Suppose further that $f_1 = \sum f_1^\gamma$ with $f_1^\gamma \in \mathcal{M}(\Gamma_{01}(p^{r+1}, N), \omega^\gamma, k_1)$ a p-adic modular form of level N and weight $(k_1, k_1+\gamma)$. Finally, suppose that if $f_2 = \sum f_2^\gamma$ with $f_2^\gamma \in \mathcal{A}(\Gamma_{01}(p^{r+1}, N), \omega^\gamma, k_2)$, then the q-expansion at $i\infty$ of each f_3^γ is a p-adic modular form of level N and weight $(k_3, k_3+\gamma)$. Indeed $(k_2, k_2+\gamma)$. Then we claim that if $f_3 = \sum f_3^\gamma$ with

$$f_3^\gamma \in \mathcal{M}(\Gamma_{01}(p^{r+1}, N), \omega^\gamma, k_3),$$

each f_3^γ is a p-adic modular form of level N and weight $(k_3, k_3+\gamma)$. Indeed,

$$f_3 = \sum_{\gamma=1}^{p-1} \sum_{\gamma_1+\gamma_2 \equiv \gamma \,(p-1)} f_1^{\gamma_1} f_2^{\gamma_2}$$

with

$$\sum_{\gamma_1+\gamma_2 \equiv \gamma \,(p-1)} f_1^{\gamma_1} f_2^{\gamma_2} \in \mathcal{A}(\Gamma_{01}(p^{r+1}, N), \omega^\gamma, k_3),$$

and by the uniqueness of character decomposition,

$$f_3^\gamma = \textstyle\sum_{\gamma_1+\gamma_2 \equiv \gamma \,(p-1)} f_1^{\gamma_1} f_2^{\gamma_2}.$$

From the suppositions, $f_1^{\gamma_1} f_2^{\gamma_2}$ is a p-adic modular form of level N and weight $(k_1+k_2, k_1+k_2+\gamma_1+\gamma_2)$, so $f_3^\gamma \in \bar{\mathcal{M}}(\Gamma(N), (k_3, k_3+\gamma))$.

It is now possible to assume $S(r)$ and prove $S(r+1)$. Since

$$\mathcal{M}(\Gamma_{01}(p^{r+1}, N), k) = \bigoplus \mathcal{M}(\Gamma_{01}(p^{r+1}, N), \xi, k),$$

it is enough to verify $S(r+1)$ for $f \in \mathscr{M}(\Gamma_{01}(p^{r+1}, N), \xi, k)$. Let $t = 4(p-1)$, $f_1 = (f)E_t(q^{p^{r-1}}, \bar{\xi}), f_2 = E_{-t}(q^{p^{r-1}}, \bar{\xi})$. Then the hypotheses of the preceding paragraph hold for $f_1 \in \mathscr{M}(\Gamma_{01}(p^r, N), k+t)$ by $S(r)$ while they hold for f_2 by Proposition 11. Hence the desired conclusion holds for $f_3 = f_1 f_2 = f$: $f = \sum_{\gamma=1}^{p-1} f^\gamma$ with $f^\gamma \in \mathscr{M}(\Gamma_{01}(p^{r+1}, N), \omega^\gamma, k)$ a p-adic modular form of level N and weight $(k, k+\gamma)$.

4. p-adic L-functions

Using Theorem 12, we can deduce a "constant term theorem" for certain forms on $\Gamma_1(p^r, N)$, which will in turn be used to establish the existence of p-adic abelian L-functions. First recall that there is a natural decomposition $(\mathbf{Z}/p^r\mathbf{Z})^\times \simeq (\mathbf{Z}/p\mathbf{Z})^\times \oplus (\mathbf{Z}/p^{r-1}\mathbf{Z})$, $p \neq 2$. Correspondingly, any character χ on $(\mathbf{Z}/p^r\mathbf{Z})^\times$ may be expressed uniquely as $\chi = \chi_1\chi_2$, where χ_1 is a character of $(\mathbf{Z}/p\mathbf{Z})^\times$ and χ_2 is a character of $(\mathbf{Z}/p^{r-1}\mathbf{Z})$. Two lemmas will be needed, the first of which is a restatement of known results on generalized Bernoulli numbers.

Lemma 13 *Let $\chi = \chi_1\chi_2$ be a character of $(\mathbf{Z}/p^r\mathbf{Z})$, $p \neq 2$. Suppose $k \in \mathbf{N}$, $\chi_1 = \omega^j$ and $(p-1)\,|\,(j+k)$. Then:*

(1) *if $\chi_2 = 1$, $v_p(B_\chi^k/k) = -1 - v_p(k)$;*

(2) *if $\chi_2 \neq 1$, $v_p(B_\chi^k/k) = -1/(p-1)p^{m-2}$ where p^m is the conductor of χ.*

Proof If v is an integer not divisible by p, write $v = \omega(v)\langle v\rangle$. If $\chi_1 = \chi_2 = 1$, the lemma is a special case of the theorem of Clausen–Von Staudt. Otherwise, consider the ideal $\mathfrak{p} = (p, 1 - \chi(g)g^k)$ in $\mathbf{Q}(\zeta_{(p-1)p^r})$, where g is a primitive root mod p. Then $\mathfrak{p} = (p, 1 - \omega(g)^j\chi_2(g)\omega(g)^k\langle g\rangle^k) = (p, 1 - \chi_2(g)\langle g\rangle^k) \neq (1)$, since $\chi_2(v)$ is a p^rth root of unity and $v_p(\langle v\rangle - 1) > 0$ for all v. If $\chi_2 = 1$, Theorem 3 of [1] thus implies $pB_\chi^k \equiv (p-1) \bmod \mathfrak{p}$, so $v_p(pB_\chi^k) = 0$ and $v_p(B_\chi^k/k) = -1 - v_p(k)$. On the other hand, if $\chi_2 \neq 1$, the same theorem states $(1 - \chi(1+p))B_\chi^k/k \equiv 1 \bmod \mathfrak{p}$. Since χ is of conductor p^m, $\chi(1+p) = \chi_2(1+p)$ must be a *primitive* (p^{m-1})th root of unity, so $v_p(B_\chi^k/k) = -v_p(1 - \chi(1+p)) = -1/(p-1)p^{m-2}$.

Lemma 14 *For $\chi = \omega^j\chi_2$ a character of $(\mathbf{Z}/p^r\mathbf{Z})^\times$, $p \neq 2$, let*

$$\tilde{\phi}_k(\chi) = \sum_{n=1}^{\infty} \sum_{v|n} \tilde{\chi}(v)\tilde{v}^{k-1}q^n.$$

If $(p-1)\,|\,(k+j)$, then $\tilde{\phi}_k(\chi) \notin \tilde{\mathscr{M}}(\Gamma_1(p^r, N), \chi, k)$. (Here the summation is over positive v.)

Choose an integer l large enough so that $m = (p-1)p^l - k \geq 4$. Since $v_p(E_m(\bar{\chi}) - 1) > 0$, $\tilde{\phi}_k(\chi) \in \tilde{\mathscr{M}}(\Gamma_1(p^r, N), \chi, k)$ would imply $\tilde{\phi}_k(\chi) =$

$\tilde{\phi}_k(\chi)\tilde{E}_m(\bar{\chi}) \in \tilde{\mathcal{M}}(\Gamma_0(p^r, N), (p-1)p^l)$. Letting $s = (p-1)p^l$,

$$\tilde{\chi}(v)\tilde{v}^{k-1} = \tilde{\omega}(v)^j\tilde{\chi}_2(v)\tilde{\omega}(v)^{k-1}\langle\tilde{v}\rangle^{k-1} = \tilde{\omega}(v)^{j+k-1} = \tilde{\omega}(v)^{s-1}.$$

Hence $\tilde{\phi}_k(\chi) = \tilde{\phi}_s(1)$, and it suffices to show

$$\tilde{\phi}_s = \tilde{\phi}_s(1) = \sum_{n=1}^{\infty}\sum_{v|n}\tilde{v}^{k-1}q^n \notin \mathcal{M}(\Gamma_0(p^r, N), s).$$

Assume the contrary, i.e., $\tilde{\phi}_s \in \tilde{\mathcal{M}}(\Gamma_0(p^r, N), s)$. By Theorem 12 any modular form on $\Gamma_0(p^r, N)$ may be approximated by forms on $\Gamma(N)$. In particular, $\tilde{\phi}_s \in \tilde{\mathcal{M}}(\Gamma(N), t)$ with $s \equiv t \bmod (p-1)$ and $t \geq 4$, which in turn implies $\tilde{\phi}_t \in \tilde{\mathcal{M}}(\Gamma(N), t)$. If ϕ_t has reduction $\tilde{\phi}_t$ and $G_k = -B_k/2k + \sum_{n=1}^{\infty}\sum_{v|n} v^{k-1}q^n$, then $f = G_t - \phi_t \in \mathcal{M}(\Gamma(N), t)$. However, $v_p(a_0(f)) = v_p(a_0(G_t)) = -1 - v_p(t)$ while $\inf_{n\geq 1} v_p(a_n(f)) > 0$. Therefore,

$$v_p(a_0(f)) < \inf_{n\geq 1} v_p(a_n(f)) - v_p(t) - 1,$$

contradicting Corollary C.

Theorem 15A *Suppose χ is a character of $(\mathbf{Z}/p^r\mathbf{Z})^\times$, $p \neq 2$, with conductor p^m and $\chi_1 = \omega^j$. Let*

$$f = \sum_{n=0}^{\infty} a_n q^n \in \mathcal{M}(\Gamma_1(p^r, N), \chi, k).$$

(1) *If $(p-1) \nmid (k+j)$, then $v_p(a_0) \geq \inf_{n\geq 1} v_p(a_n)$.*

(2) *If $(p-1)\,|\,(k+j)$ and $\chi_2 = 1$, then $v_p(a_0) \geq \inf_{n\geq 1} v_p(a_n) - v_p(k) - 1$.*

(3) *If $(p-1)\,|\,(k+j)$ and $\chi_2 \neq 1$, then $v_p(a_0) \geq \inf_{n\geq 1} v_p(a_n) - 1/(p-1)p^{m-2}$.*

Proof Suppose (1) is not true, so we may take $a_0 = 1$ and $\inf_{n\geq 1} v_p(a_n) > 0$, i.e., $f = 1 + \pi\sum_{n=1}^{\infty} c_n q^n$, π a uniformizer for a field of definition of f. Then $f^{p^r} \equiv 1 \bmod \pi$, that is to say, $v_p(a_0(f^{p^r})) > \inf_{n\geq 1} v_p(a_n(f^{p^r}))$. Since the values taken by χ and χ_2 are respectively $(p-1)$th and p^rth roots of unity, $\chi_1^{p^r} = \chi_1$, while $\chi_2^{p^r} = 1$. Hence $f^{p^r} \in \mathcal{M}(\Gamma_{01}(p^r, N), \omega^j, p^r k) \subset \bar{\mathcal{M}}(\Gamma(N), (p^r k, k+j))$ by Theorem 12. The fact that $v_p(a_0(f^{p^r})) > \inf_{n\geq 1} v_p(a_n(f^{p^r}))$ is therefore a contradiction to Corollary C.

Case (2) follows directly from Theorem 12 and Corollary C. Finally, suppose (3) is not true, so we may take $a_0 = 1$, $\inf_{n\geq 1} v_p(a_n) > 1/(p-1)p^{m-2}$, and $k \geq 4$, after replacing f by $f \cdot E_{2(p-1)}$ if necessary. Let $g = L(1-k, \chi)f$, so $a_0(g) = L(1-k, \chi)$ while $\inf_{n\geq 1} v_p(a_n(g)) > 0$ by Lemma 13. Therefore, $\tilde{\phi}_k = (G_k(\chi) - g)\tilde{}/2 \in \tilde{\mathcal{M}}(\Gamma_1(p^r, N), \chi, k)$, which contradicts Lemma 14.

There is also a decomposition of $(\mathbf{Z}/p^r\mathbf{Z})^\times$ for $p = 2$, namely $(\mathbf{Z}/2^r\mathbf{Z})^\times \simeq (\mathbf{Z}/2^2\mathbf{Z})^\times \oplus (\mathbf{Z}/2^{r-2}\mathbf{Z})$. And there is a corresponding decomposition

$\chi = \chi_1 \chi_2$ of any character χ of $(\mathbf{Z}/2^r\mathbf{Z})^\times$. For $p = 2$, ω previously represented the trivial character of $(\mathbf{Z}/2\mathbf{Z})^\times$. Henceforward, let ω instead represent the nontrivial character of $(\mathbf{Z}/2^2\mathbf{Z})^\times$, so $\chi_1 = \omega^1$ or ω^2. As an analogue of Theorem 15A, we have for $p = 2$:

Theorem 15B *Suppose χ is a character of $(\mathbf{Z}/2^r\mathbf{Z})^\times$ with $\chi_1 = \omega^j$. Let*

$$f = \sum_{n=0}^{\infty} a_n q^n \in \mathcal{M}(\Gamma_1(2^r, N), \chi, k).$$

(1) *If $2 \nmid (k + j)$, then $v_p(a_0) \geq \inf_{n \geq 1} v_p(a_n)) - v_p(k) - 2$.*
(2) *If $2 \mid (k + j)$ and $\chi_2 = 1$, then $v_p(a_0) \geq \inf_{n \geq 1} v_p(a_n) - v_p(k) - 2$.*
(3) *If $2 \mid (k + j)$ and $\chi_2 \neq 1$, then $v_p(a_0) \geq \inf_{n \geq 1} v_p(a_n) - 1/2^{m-3}$, 2^m the conductor of χ.*

Proof If (1) or (2) is wrong, we may assume $v_p(f - 1) > v_p(k) + 2$. Then $f^{p^r} \in \mathcal{M}(\Gamma_0(p^r, N), p^r k)$ satisfies $v_p(f^{p^r} - 1) > v_p(k) + 2 + r$, or

$$v_p(a_0(f^{p^r})) < \inf_{n \geq 1} v_p(a_n(f^{p^r})) - v_p(p^r k) - 2,$$

which contradicts Corollary C.

To prove (3), we begin by showing $v_p(a_0) \geq \inf_{n \geq 1} v_p(a_n) - 1$. First observe that

$$\tilde{\phi}_k(\chi) = \sum_{n=1}^{\infty} \sum_{v \mid n} \tilde{\chi}(v) \tilde{v}^{k-1} q^n \notin \tilde{\mathcal{M}}(\Gamma_1(p^r, N), \chi, k).$$

Indeed, if the contrary held,

$$\tilde{\phi}_k(\chi)^{p^r} = \textstyle\sum_{n=1}^{\infty} \sum_{v \mid n} \tilde{v}^{k-1} q^{p^r n} \in \tilde{\mathcal{M}}(\Gamma_0(p^r, N), p^r k),$$

which implies $\tilde{\phi}_t^{p^r} \in \tilde{\mathcal{M}}(\Gamma(N), t)$ for some even $t \geq 4$. Then $f = G_t \mid V^r - \phi_t^{p^r} \in \tilde{\mathcal{M}}(\Gamma(N), t)$ and $v_p(a_0(f)) < \inf_{n \geq 1} v_p(a_n(f)) - v_p(t) - 2$, a contradiction to Corollary C. Now if $g \in \mathcal{M}(\Gamma_1(p^r, N), \chi, k)$ is such that $v_p(a_0) < \inf_{n \geq 1} v_p(a_n) - 1$, we may take $k \geq 4$ and $v_p(g - 1) > 1$. By Theorem 3 of [1], $v_p(L(1 - k, \chi)) \geq 0$, so

$$\tilde{\phi}_k(\chi) = (G_k(\chi)/2 - L(1 - k, \chi)g/2)^{\sim} \in \tilde{\mathcal{M}}(\Gamma_1(p^r, N), \chi, k),$$

violating the previous observation.

To show that in fact $v_p(a_0) \geq \inf v_p(a_n) - 1/p^{m-3}$, suppose $f \in \mathcal{M}(\Gamma_1(p^r, N), \chi, k)$, $v_p(f - 1) > 1/p^{m-3}$ with χ of conductor p^m, $m \geq 3$. Then $v_p(f^{p^{m-3}} - 1) > 1$ with $f^{p^{m-3}} \in \mathcal{M}(\Gamma_1(p^r, N), \chi^{p^{m-3}}, p^{m-3}k)$, which is impossible because $(\chi^{p^{m-3}})_2 \neq 1$.

It should be possible to replace the conclusion of Theorem 15B(1) with $v_p(a_0) \geq \inf v_p(a_n) - 1$, completing the analogy with 15A(1). However, we have not been able to prove this if χ has conductor 8. Theorem 15A has the

important consequence that if χ has conductor p^m *with* $m > 1$ ($p \neq 2$), then $v_p(a_0) \geq \inf_{n \geq 1} v_p(a_n) - \lambda$ *with* λ *independent of* k. This phenomenon is related to the fact that modular forms on $\Gamma_0(p^r, N)$ with such a character need *not* be p-adic modular forms of level N.

The next theorem, an analogue of Corollary D, is the final payoff of our theory of forms on $\Gamma_0(p^r, N)$. It provides the necessary power to establish the existence of p-adic abelian L-functions.

Theorem 16 *Let*

$$f^{(i)} = \sum_{n=0}^{\infty} a_n^{(i)} q^n \in \mathcal{M}_K(\Gamma_1(p^r, N), \chi^{(i)}, k_i), \qquad i = 1, 2, \ldots.$$

If $p \neq 2$, *suppose each* $\chi^{(i)} = \omega^{(j_i)}\chi$, *with* χ *a fixed character of* $(\mathbf{Z}/p^{r-1}\mathbf{Z})$. *If* $p = 2$, *suppose each* $\chi^{(i)} = \chi$, *a fixed character of* $(\mathbf{Z}/p^r\mathbf{Z})^\times$, *and write* $j_i = 0$ *for each* i. *Finally, suppose that the* $a_n^{(i)}$ *tend uniformly toward* a_n *for* $n \geq 1$, *and the* $(k_i, k_i + j_i)$ *approach a limit in* X, *nonzero if* $\chi = 1$ *or* $p = 2$. *Then the* $a_0^{(i)}$ *approach a limit* a_0.

Proof After replacing each $f^{(i)}$ by $f^{(i)}E_{(p-1)p^i + j_i}(\bar{\omega}^{j_i})$, we may assume $f^{(i)} \in \mathcal{M}_K(\Gamma_1(p^r, N), \chi, k_i)$ for a fixed character χ. The $a_n^{(i)}$ still converge uniformly for $n \geq 1$, and the k_i approach a limit in X, nonzero if $\chi = 1$ or $p = 2$. The proof is now the same as that of Corollary D, with Theorem 15 replacing Corollary C.

We now take as our object of study p-adic abelian L-functions. Henceforth, let K be any totally real number field, L any abelian extension of K, and G the Galois group of L over K. If χ is a character of G, there exists an ideal $\mathfrak{f}$ of K called the conductor of χ, such that χ induces a character on the ray class group $R_\mathfrak{f} = I_\mathfrak{f}/P_\mathfrak{f}$. Here $I_\mathfrak{f}$ is the set of ideals of K prime to $\mathfrak{f}$, and

$$P_\mathfrak{f} = \{(\alpha) \in I_\mathfrak{f} \mid \alpha \in K, \alpha \gg 0, \alpha \equiv 1 \bmod \mathfrak{f}\}.$$

Conversely, by class field theory, if $\mathfrak{f}$ is any K-ideal and χ a character of $R_\mathfrak{f}$, then χ comes from a character of some abelian extension of K.

If $\bar{\mathfrak{f}}$ is the least common multiple of $\mathfrak{f}$ and (p), then *a fortiori* χ induces a character of $R_{\bar{\mathfrak{f}}}$. For $s > 1$, an abelian L-function is defined by $L_T^S(\chi, s) = \sum_{\mathfrak{a} \in I_\mathfrak{f}} \chi(\mathfrak{a})^{-s}$ where the summation is over all integral ideals and $I_\mathfrak{f}$ and N denotes the norm from K to $\mathbf{Q}$. $L_K^S(\chi, s)$, or simply $L(\chi, s)$, has an analytic continuation to the whole plane, with a possible pole at $s = 1$, and has a functional equation. As observed by Klingen [5], the values of $L(\chi, s)$ at negative integers s are contained in the same finite extension of $\mathbf{Q}$ as the values of χ. It therefore is meaningful to define a "p-adic abelian L-function" from $\mathbf{Z}_p$ to Ω_p by p-adic interpolation. In order to be more precise, let θ be the character of $R_\mathfrak{f}$ defined by $\omega(N\mathfrak{a})$ and discussed below. Let $d = [K(\xi) : K]$ where $\zeta = \zeta_p$ if $p \neq 2$ and $\zeta = \zeta_4$ if $p = 2$.

Theorem 17 *Let K be a totally real number field, L an abelian extension of K, and χ a character of* $\mathrm{Gal}(L/K)$. *Then there exists a unique continuous function $L_p(\chi, s)$ from $\mathbf{Z}_p$ to Ω_p, possibly undefined at $s = 1$, such that $L_p(\chi, 1-n) = L_K^S(\chi\theta^{-n}, 1-n)$ for $n \in \mathbf{N}$. In particular, at any negative integer $s \equiv 1 \bmod d$, $L_p(\chi, s) = L_K^S(\chi, s)$.*

Proof Let us first consider the character θ, following [2]. Denoting the abelian extension $L(\zeta)$ of K by L_0, define a character, also written θ, of $G_0 = \mathrm{Gal}(L_0/K)$ as follows: If $\rho \in G_0$, choose an ideal $\mathfrak{r} \in I_{\mathfrak{f}}$ such that $\rho = (\mathfrak{r}, L_0/K)$ and let $\theta(\rho) = \omega(N\mathfrak{r})$. This is well defined because upon restricting to $\mathbf{Q}(\zeta)$, $(\mathfrak{r}, L_0/K) = \rho = (\mathfrak{r}', L_0/K)$ implies $(N\mathfrak{r}, \mathbf{Q}(\zeta)/\mathbf{Q}) = (N\mathfrak{r}', \mathbf{Q}(\zeta)/\mathbf{Q})$, which implies $\omega(N\mathfrak{r}) = \omega(N\mathfrak{r}')$. Since this new character of G_0 clearly induces θ on $I_{\mathfrak{f}}$ and $(p)|\mathfrak{f}$, θ *is* a ray class character of R. Moreover, $(\mathfrak{r}, K(\zeta)/K)^d = 1$ so $(N\mathfrak{r}, \mathbf{Q}(\zeta)/\mathbf{Q})^d = 1$ and $\theta(\rho)^d = \omega(N\mathfrak{r})^d = 1$. Thus $L_p(\chi, 1-n) = L(\chi\theta^{-n}, 1-n)$ for all $n \in \mathbf{N}$ gives $L_p(\chi, 1-n) = L(\chi, 1-n)$ for $n \equiv 0 \bmod d$, i.e., the second assertion of the theorem is a special case of the first. Finally, for use below, note that if σ is any embedding of L_0 into $\mathbf{C}$ and γ is complex conjugation, then $\theta(\sigma^{-1}\gamma\sigma) = -1$ because $\sigma^{-1}\gamma\sigma(\zeta) = \zeta^{-1}$.

Since there is a natural map $\mathrm{Gal}(L_0/K) \to \mathrm{Gal}(L/K)$, χ can be viewed as a character on G_0 without changing the induced character on $R_{\mathfrak{f}}$ or the function $L_K^S(\chi, s)$. First, suppose that χ is *not* real, that is, for some embedding σ of L_0 into $\mathbf{C}$, $\chi(\sigma^{-1}\gamma\sigma) = -1$. Whether n is even or odd, the Γ-factor in the functional equation of $L(\chi\theta^{-n}, s)$ corresponding to σ then has a pole at $1-n$, and $L(\chi\theta^{-n}, 1-n)$ is always zero. Hence, if χ is not real, $L_p(\chi, s) = 0$ satisfies the conditions of the theorem. And whether or not χ is real, $L_p(\chi, s)$ is unique because the negative integers are dense in $\mathbf{Z}_p$.

Now suppose that χ *is* real, so the generalized conductor of χ contains no infinite primes. Then $\chi((\alpha)) = 1$ for $\alpha \in K$, $\alpha \equiv 1 \bmod \mathfrak{f}$; and $\chi\theta^{-n}((\alpha)) = (\mathrm{sgn}\, N\alpha)^n$ for such an α and any $n \in \mathbf{N}$. If $(f) = \mathbf{Z} \cap \mathfrak{f}$, $f > 0$, then $\chi\theta^{-n}$ induces a Dirichlet character modulo f, also denoted $\chi\theta^{-n}$, in a natural fashion. Moreover, by a theorem of Kloosterman–Siegel [10],

$$G_K^k(\chi\theta^{-n}) = L(\chi\theta^{-n}, 1-k) + 2^\tau \sum_{n=1}^{\infty} \sum_{x,\mathfrak{a}} \chi(\mathfrak{a})(N\mathfrak{a})^{k-1} q^n \in \mathscr{M}(\Gamma_1(f), \chi\theta^{-n}, \tau k)$$

if n and k have the same parity. Here $\tau = [K : \mathbf{Q}]$ and the inner summation is over pairs $(x, \mathfrak{a})$ with $\mathfrak{a} \in I$, $x \in \mathfrak{d}^{-1}\mathfrak{a}$, $x \gg 0$, and $\mathrm{Tr}\, x = n$. Writing $f = p^r N$ with $p \nmid N$, $\chi\theta^{-n}$ induces a character of $(\mathbf{Z}/p^r\mathbf{Z})^\times$, and $G_K^k(\chi\theta^{-n}) \in \mathscr{M}(\Gamma_1(p^r, N), \chi\theta^{-n}, \tau k)$.

For χ real, first suppose $p \neq 2$. Given $s \in \mathbf{Z}_p$, $s \neq 0$, choose a sequence of positive integers k_i approaching s such that $(p-1)|k_i$. As $i \to \infty$, the non-

constant terms of the $G_K^{k_i}(\chi)$ uniformly approach limits, specifically,

$$\sum_{\mathrm{Tr}\, x = n} \chi(\mathfrak{a}) N(\mathfrak{a})^{k_i - 1} \to \sum_{\mathrm{Tr}\, x = n} \chi(\mathfrak{a}) \omega(N\mathfrak{a})^{-1} \langle N\mathfrak{a} \rangle^{s-1}.$$

Therefore, by Theorem 16, the constant terms $L(\chi, 1 - k_i)$ also approach a limit, call it $L_p(\chi, 1 - s)$. Theorem 15 shows $L_p(\chi, 1 - s)$ is a continuous function of s because if $v_p(k_i^{(2)} - k_i^{(1)})$ is large, so is

$$\inf_{n \geq 1} v_p(a_n(G_K^{k_i^{(2)}}(\chi) - G_K^{k_i^{(1)}}(\chi) E_{k_i^{(2)} - k_i^{(1)}})).$$

Thus it only remains to show $L_p(\chi, 1 - n) = L(\chi\theta^{-n}, 1 - n)$ for $n \in \mathbf{N}$. If $k_i \to n$ with $(p-1) | k_i$, then $\sum \chi(\mathfrak{a}) N(\mathfrak{a})^{k_i - 1} \to \sum \chi(\mathfrak{a}) \theta(\mathfrak{a})^{-1} \langle N\mathfrak{a} \rangle^{n-1} = \sum \chi\theta^{-n}(\mathfrak{a}) N(\mathfrak{a})^{n-1}$. Since $N(x\mathcal{O}_K) = (x)^\tau$ for $x \in \mathbf{Z}$, the character induced by θ on $(\mathbf{Z}/p^r\mathbf{Z})^\times$ is ω^τ. Hence

$$f_i = G_K^{k_i}(\chi) - G_K^n(\chi\theta^{-n}) E_{\tau(k_i - n)}(\omega^{\tau n}) \in \mathcal{M}(\Gamma_1(p^r, N), \chi, \tau k_i),$$

and applying Theorem 15 to f_i as $i \to \infty$ gives the desired result.

Finally, suppose χ is real and $p = 2$. Given a nonzero $s \in \mathbf{Z}_p$, choose $k_i \to s$, the k_i necessarily even if $s \in 2\mathbf{Z}_2$ and necessarily odd if $s \notin 2\mathbf{Z}_2$. By the same reasoning as above, the constant terms of $G_K^{k_i}(\chi)$, respectively $G_K^{k_i}(\chi\theta^{-1})$, approach a limit if $s \in 2\mathbf{Z}_2$, respectively $s \notin 2\mathbf{Z}_2$. Moreover, as above, if this limit is denoted $L_p(\chi, 1 - s)$, then $L_p(\chi, 1 - n) = L(\chi\theta^{-n}, 1 - n)$. $L_p(\chi, 1 - n)$ is continuous on $2\mathbf{Z}_2 - \{0\}$ and on $\mathbf{Z}_2 - 2\mathbf{Z}_2$, so it is indeed continuous on all of $\mathbf{Z}_2 - \{0\}$.

Theorem 18 *If the Dirichlet character induced by χ has conductor divisible by p, then $L_p(\chi, s)$ is defined at $s = 1$ $(p \neq 2)$.*

Proof If the p-conductor part of the induced character is $\omega^j \chi_2^{(p)}$, then either $j \neq 0$ or $\chi_2^{(p)} \neq 1$. Theorem 15A(1) or 15A(3) may then be used to establish the convergence of $L(\chi, 1 - k_i)$, $k_i \to 0$, as above.

Theorem 18 should remain true under the weaker hypothesis that the Dirichlet character induced by χ is nontrivial. Indeed, $L_p(\chi, s)$ is probably defined at $s = 1$ if and only if χ itself is nontrivial, but the proof of this no doubt requires more advanced techniques.

REFERENCES

[1] L. Carlitz, Arithmetic properties of generalized Bernoulli numbers, *J. Reine Angew. Math.* **202** (1959), 174–182.

[2] J. Coates and W. Sinnott, On p-adic L-functions over real quadratic fields, *Invent. Math.* **25** (1974), 253–279.

[3] K. Iwasawa, "Lectures on p-adic L-functions." Princeton Univ. Press, Princeton, New Jersey, 1972.

[4] N. Katz, "P-adic properties of modular schemes and modular forms," International Summer School at Antwerp, 1972. Lecture Notes in Math. 350, pp. 70–190, Springer-Verlag, Berlin and New York, 1973.
[5] H. Klingen, Über die Werte der Dedekindschen Zetafunction, *Math. Ann.* **145** (1962), 265–272.
[6] T. Kubota and H. W. Leopoldt, Eine p-adische Theorie der Zetaverte, *J. Crelle* (1964), 214–215, 328–339.
[7] D. H. Lehmer, Some properties of circulents, *J. Number Theory* **5** (1973), 43–54.
[8] A. Ogg, "Modular Forms and Dirichlet Series." Benjamin, New York, 1969.
[9] J.-P. Serre, "Congruences et formes modulaires," Séminaire N. Bourbaki, Exposé 416, 1971–1972; Lecture Notes in Math. 317, pp. 319–338, Springer-Verlag, Berlin and New York, 1973.
[10] J.-P. Serre, "Formes modulaires et fonctions zeta p-adiques." International Summer School at Antwerp, 1972. Lecture Notes in Math. 350, pp. 191–268, Springer-Verlag, Berlin and New York, 1973.
[11] C. L. Siegel, Über die Fourierschen Koeffizienten von Modulformen, *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II* **3** (1970), 15–56.
[12] H. P. F. Swinnerton-Dyer, On l-adic representations and congruences for coefficients of modular forms. International Summer School at Antwerp, 1972; Lecture Notes in Math. 350, pp. 3–55, Springer-Verlag, Berlin and New York, 1973.

AMS (MOS) 1970 subject classification: 12A70.

A Characterization of the Line–Hyperplane Design of a Projective Space and Some Extremal Theorems for Matroid Designs†

D. K. RAY-CHAUDHURI *N. M. SINGHI*

THE OHIO STATE UNIVERSITY
COLUMBUS, OHIO

Combinatorial characterizations of some incidence structures obtained from projective spaces and affine spaces over finite fields are given. Also some extremal theorems for matroid designs are proved.

1. Introduction

An incidence structure is a triple $(X, \mathscr{B}, I)$, X and $\mathscr{B}$ are finite sets, and $I \subseteq X \times \mathscr{B}$. Elements of X are called treatments, while elements of $\mathscr{B}$ are called blocks. If $(x, B) \in I$, we say that x is incident with B, and denote it by $x \in B$. We shall follow the usual notations of incidence structures, and often consider a block as the set of treatments incident with it. If D and D' are isomorphic incidence structures, we write $D \simeq D'$. For any $B \in \mathscr{B}$, we shall

† This research was supported in part by NSF grant MPS 75-08231 and ONR contract N00014-67-A-0232-0016.

denote by $|B|$ the number of treatments incident with it. Incidence structures are also called designs; for various definitions connected with incidence structures, see Dembowski [4].

An incidence structure $D = (X, \mathscr{B}, I)$ is said to be BIBD (v, b, r, k, λ) iff (if and only if) it satisfies following conditions:

(a) $|X| = v$, $|\mathscr{B}| = b$.
(b) $|B| = k$ for all $B \in \mathscr{B}$.
(c) Each treatment is incident with exactly r blocks.
(d) Every pair of treatments is incident with exactly λ blocks.

Parameters (v, b, r, k, λ) satisfy the equations

$$\lambda(v-1) = r(k-1) \tag{1.1}$$

$$bk = rv \tag{1.2}$$

$$b \geq v \text{ (Fisher's inequality).} \tag{1.3}$$

A BIBD (v, b, r, k, λ) with $v = b$ and hence $r = k$ is called an SBIBD (v, k, λ). For further results on BIBDs, see [4].

An incidence structure $G = (X, \mathscr{B}, I)$ is called a simple graph iff $|B| = 2$ for each $B \in \mathscr{B}$, and if $B_1, B_2 \in \mathscr{B}$, $B_1 \neq B_2$, B_1 and B_2 are distinct treatment sets. Treatments of a graph are also called vertices, while blocks are called edges. Two vertices x and y are said to be adjacent iff there exists an edge incident with both x and y. A simple graph $G = (X, \mathscr{B}, I)$ is said to be a strongly regular graph $G(v, n_1, p_{11}^1, p_{11}^2)$ [2], iff it satisfies the following conditions:

(A) $|X| = v$.
(B) Each vertex is incident with exactly n_1 vertices.
(C) If $x, y \in X$, $x \neq y$, there are exactly p_{11}^1 or p_{11}^2 vertices z such that z is adjacent to both x and y according as x and y are adjacent or not adjacent.

Let X be a set of v elements and $G = G(v, n_1, p_{11}^1, p_{11}^2)$ be a strongly regular graph with vertex set X. An incidence structure $D = (X, \mathscr{B}, I)$ is called a PBIBD $(v, b, r, k, \lambda_1, \lambda_2)$, with association graph $G(v, n_1, p_{11}^1, p_{11}^2)$ iff following conditions are satisfied:

(i) $|X| = v$, $|\mathscr{B}| = b$.
(ii) $|B| = k$ for each $B \in \mathscr{B}$.
(iii) Each treatment is incident with exactly r blocks.
(iv) Any two distinct treatments x and y occur together in exactly λ_1 or λ_2 blocks of D according as x and y are adjacent or not adjacent in G.

We shall denote the association graph of a PBIBD D by $G(D)$. For various examples and results on PBIBDs, see [4]. We shall denote by

$PG(d, q)$, a projective space of dimension d over a finite field $GF(q)$, while by $AG(d, q)$ we shall denote a d-dimensional affine space over $GF(q)$.

For $d > m > l \geq 0$, define an incidence structure $P_{l,m}(d, q)$ as follows. Treatments of $P_{l,m}(d, q)$ are all l-dimensional subspaces of $PG(d, q)$. An incidence relation is given by containment. $A_{l,m}(d, q)$ is similarly defined by taking $AG(d, q)$ instead of $PG(d, q)$. When no confusion arises we shall also write $P_{l,m}$ for $P_{l,m}(d, q)$ and $A_{l,m}$ for $A_{l,m}(d, q)$. The following results are well known and can be proved easily by using common properties of projective and affine spaces:

(a) $P_{0,m}(d, q)$ and $A_{0,m}(d, q)$ are BIBDs for all $d > m > 0$. (1.4)

(b) If $d \geq 3$, $P_{1,d-1}(d, q)$ is a PBIBD $(v, b, r, k, \lambda_1, \lambda_2)$, where

$$v = \frac{(q^{d+1}-1)(q^d-1)}{(q^2-1)(q-1)}, \qquad b = \frac{q^{d+1}-1}{q-1}, \qquad r = \frac{q^{d-1}-1}{q-1}$$

$$k = \frac{(q^d-1)(q^{d-1}-1)}{(q^2-1)(q-1)}, \qquad \lambda_1 = \frac{q^{d-2}-1}{q-1}, \qquad \lambda_2 = \frac{q^{d-3}-1}{q-1} \tag{1.5}$$

$G(P_{1,d-1})$ is a strongly regular graph $(v, n_1, p_{11}^1, p_{11}^2)$ where

$$n_1 = (q+1)q\left(\frac{q^{d-1}-1}{q-1}\right), \qquad p_{11}^1 = \frac{q^d-1}{q-1} - 2 + q^2$$

$$p_{11}^2 = (q+1)^2. \tag{1.6}$$

Any two vertices in $G(P_{1,d-1})$ are joined by an edge iff they are intersecting lines in $PG(d, q)$.

By "replacing" a desarguesian plane by nondesarguesian plane in $PG(d, q)$ or $AG(d, q)$ one can construct BIBDs, with the same parameters as those of $P_{0,m}$ or $A_{0,m}$, but nonisomorphic to $P_{0,m}$ or $A_{0,m}$, respectively (see, for example, Mavron [8]). Dembowski and Wagner [5] proved a characterization theorem for $P_{0,d-1}(d, q)$ for $d \geq 3$. In Section 3 we prove the following characterization theorem for $P_{1,d-1}(d, q)$ for $d \geq 6$.

Theorem 1 *Let d and q be positive integers, $d \geq 6, q > 1$. Suppose D_1 is a PBIBD $(v, b, r, k, \lambda_1, \lambda_2)$, where parameters are given by* (1.5), *and $G(D_1)$ has parameters $(v, n_1, p_{11}^1, p_{11}^2)$, given by Eqs.* (1.6), *then q is a prime power,*

$$D_1 \simeq P_{1,d-1}(d, q) \qquad \textit{and} \qquad G(D_1) \simeq G(P_{1,d-1}).$$

We define a combinatorial geometry (or matroid) by the "hyperplane axioms." An incidence structure $D = (X, \mathscr{B}, I)$, is said to be a combinatorial geometry iff it satisfies following conditions:

(a) Given $H_1, H_2 \in \mathscr{B}$, $H_1 \neq H_2$, H_1 is not a proper subset of H_2.

(b) Given $H_1, H_2 \in \mathscr{B}$, $H_1 \neq H_2$, and $x \in X$, there exists a block $H_3 \in \mathscr{B}$, s.t. (such that) $H_1 \cap H_2 \cup \{x\} \subseteq H_3$.

(c) For each $x \in X$, $\cap H = \{x\}$, where intersection is taken over all blocks H s.t. $x \in H$.

Treatments of a combinatorial geometry are called points, while blocks are called hyperplanes. Combinatorial geometries have been studied in detail, and for various results on combinatorial geometry, we refer to Crapo and Rota [3]. We shall follow the notation of Crapo and Rota [3].

A combinatorial geometry $D = (X, \mathscr{B}, I)$ is called a geometric design iff D is also a BIBD. A regular geometric design is a combinatorial geometry in which all flats of rank i have the same cardinality m_i. It can be easily seen that a regular geometric design is indeed a geometric design [12]. Geometric designs have been studied by Edmonds, Young, and Murti [12], in particular they have given many examples of such designs. We list a few well-known examples of regular geometric designs.

(a) A $t-(v, k, \lambda)$ design [4] with $\lambda = 1$ is a regular geometric design of rank $(t+1)$ s.t.

$$m_i = i \quad \text{for} \quad 0 \leq i < t \quad \text{and} \quad m_t = k.$$

(b) $P_{0,m}$ is a regular geometric design of rank $m+1$ s.t.

$$m_i = \frac{q^i - 1}{q - 1} \qquad \text{for} \quad 0 < i \leq m < d.$$

(c) $A_{0,m}$ is a regular geometric design of rank $m+1$ s.t.

$$m_i = q^{i-1} \qquad \text{for} \quad 0 < i \leq m < d.$$

We note that $m_0 = 0$, $m_1 = 1$; and m_2 is the size of a line in any regular geometric design. Clearly $m_2 \geq 2$.

In Section 4 we shall prove the following results.

Theorem 2 *If $D = (X, \mathscr{B}, I)$ is a regular geometric design of rank $n \geq 4$, then:*

(a) $m_i - m_{i-1} \geq (m_2 - 1)(m_{i-1} - m_{i-2})$ *for* $n \geq i \geq 3$.

(b) *Equality holds in* (a) *for any i iff $D \simeq P_{0,n}(d, q)$ for some prime power q and $d \geq n+1$ or $m_2 = 2$ and D is a 3-design.*

Geometric designs of rank 3 are precisely BIBDs with $\lambda = 1$. We also study geometric designs of rank 4 in Section 4, and show that all such designs are regular and examples (a)–(c) given above are the extreme cases of certain inequalities to be satisfied.

Theorem 3 *If $D = (X, \mathscr{B}, I)$ is a regular geometric design of rank $n \geq 4$, then:*

(a) $m_i - m_j \geq (m_2 - 1)^{i-j}(m_{i-1} - m_{j-1})$ *for* $n \geq i > j \geq 2$.

(b) *Equality holds in* (a) *for any i iff $D \simeq P_{0,n}(d, q)$ for some prime power q and $d \geq n + 1$ or $m_2 = 2$ and D is a 3-design.*

Theorem 4 *Let $D = (X, \mathscr{B}, I)$ be a geometric design (v, b, r, k, λ) of rank 4, then:*

(a) $v \equiv k \bmod(\lambda - 1)$.

(b) $\lambda k - 2(\lambda - 1) \geq v \geq \lambda k - \frac{1}{2}(\lambda - 1) - \frac{1}{2}(\lambda - 1)\sqrt{4k - 3}$.

(c) $v = \lambda k - 2(\lambda - 1)$ *iff D is a 3-$(v, k, 1)$-design.*

(d) $v = \lambda k - \frac{1}{2}(\lambda - 1) - \frac{1}{2}(\lambda - 1)\sqrt{4k - 3}$ *iff* $k = q^2 + q + 1$ *for some power q and $D \simeq P_{0,2}(n, q)$ where n is given by $v = q^{n+1}/(q - 1)$ or $k \leq 7$ and D is a 3-$(v, k, 1)$-design.*

(e) *If* $v > \lambda k - \frac{1}{2}(\lambda - 1) - \frac{1}{2}(\lambda - 1)\sqrt{4k - 3}$, *then* $v \geq \lambda k - (\lambda - 1)\sqrt{k}$ *and for* $k \geq 16$ *equality holds iff $D \simeq A_{0,2}(n, q)$ where $k = q^2$ for some power q and $v = q^n$.*

2. Preliminaries

In this section we shall state various known results on characterizing geometries, which we shall be using in the next section.

Let D be a BIBD (v, b, r, k, λ) with $\lambda = 1$. It is well known that the dual D' is a PBIBD $(b, v, k, r, \lambda_1, \lambda_2)$ with $\lambda_1 = 1$, $\lambda_2 = 0$ s.t. $G(D')$ is a strongly regular graph with parameters $(b, r(k - 1), r - 2 + (k - 1)^2, k^2)$. Any two vertices B_1, B_2 are joined in $G(D')$ if and only if $|B_1 \cap B_2| = 1$ in D.

The following result is a particular case of a well-known theorem of Bose on partial geometries [2].

Proposition 5 *If $G = (V, E, I)$ is any strongly regular graph with parameters $(b, r(k - 1), r - 2 + (k - 1)^2, k^2)$, where b, r, k are integers s.t.*

$$r > \tfrac{1}{2}[k(k - 1) + k(k + 1)(k^2 - 2k + 2)]$$

then there exists a unique BIBD $D(v, b, r, k, \lambda)$ with $\lambda = 1, v = r(k - 1) + 1$ s.t. V is the set of blocks of D and $G(D') = G$.

Let $D = (X, \mathscr{B}, I)$ be an incidence structure. For $x, y \in X$, $x \neq y$, line xy is defined by

$$xy = \bigcap B$$

where intersection is taken over all blocks B s.t. $x, y \in B$.

The following well-known theorem due to Dembowski and Wagner [5] gives a characterization of the incidence structure $P_{0,d-1}(d, q)$ obtained from $PG(d, q)$.

Proposition 6 *If D is a symmetric BIBD (v, b, r, k, λ), $\lambda > 1$ s.t. its dual D' is a combinatorial geometry, then $D \simeq P_{0,d-1}(d, q)$ for some positive integer d and prime power q.*

We note that the dual D' of a BIBD $D(v, b, r, k, \lambda)$ is a combinatorial geometry iff every line of D meets every block of D.

Let $D = (X, \mathscr{L}, I)$ be an incidence structure. For each block B of D we define a new incidence structure D_B as follows. Treatments of D_B are treatments of D incident with B. Blocks of D_B are the lines of D contained in B. The following results on regular geometric designs of rank 4 are well known. The first one is essentially the definition of a projective space. The second is due to Buekenhout [1].

Proposition 7 *If D is a regular geometric design of rank 4 s.t. $m_2 \geq 3$ and D_B is a projective plane for all blocks B of D, then $D \simeq P_{0,2}(d, q)$ for some d and prime power q.*

Proposition 8 *If D is a regular geometric design of rank 4 s.t. $m_2 \geq 4$ and D_B is an affine plane for all blocks B of D, then $D \simeq A_{0,2}(d, q)$ for some d and prime power q.*

3. Proof of Theorem 1

Let d and q be positive integers, $d \geq 6$. Throughout this section we will assume that $D_1 = (X, \mathscr{B}, I)$ is a PBIBD $(v, b, r, k, \lambda_1, \lambda_2)$ with association graph $G_1(v, n_1, p_{11}^1, p_{11}^2)$, where these parameters are given by Eqs. (1.5) and (1.6). The proof of Theorem 1 is essentially based on the Propositions 5 and 6. We first prove the following simple lemma.

Lemma 9 *The dual of D_1 is a BIBD with parameters (b, v, k, r, λ) where*

$$\lambda = \frac{(q^{d-1} - 1)(q^{d-2} - 1)}{(q - 1)(q^2 - 1)}.$$

Proof We have only to prove that any two blocks of D_1 intersect in λ treatments. The following two equations are obtained easily by counting the occurrences of treatments and pairs of treatments in blocks of D_1:

$$\sum_{B_1, B_2 \in \mathscr{B}} |B_1 \cap B_2| = b(r - 1)k = vr(r - 1) \tag{3.1}$$

and

$$\sum_{B_1, B_2 \in \mathscr{B}} |B_1 \cap B_2|(|B_1 \cap B_2| - 1) = vn_1\lambda_1(\lambda_1 - 1) + v(v - 1 - n_1)\lambda_2(\lambda_2 - 1) \tag{3.2}$$

where the summations in (3.2) and (3.3) are over all pairs of distinct blocks B_1 and B_2 of D_1. Using (3.2) and (3.3) we can derive the following equation easily:

$$\sum_{B_1, B_2 \in \mathcal{B}} (|B_1 \cap B_2| - \lambda)^2 = 0. \tag{3.3}$$

From (3.3) it follows that $|B_1 \cap B_2| = \lambda$ for all blocks B_1 and B_2 of D_1, $B_1 \neq B_2$. This completes the proof.

Consider the PBIBD $D_1 = (X, \mathcal{B}, I)$. Let $l \in X$ and $B \in \mathcal{B}$. Let t_l denote the number of treatments $l_1 \in X$ s.t. $l_1 \in B$ and the vertices l and l_1 are joined in G_1. Suppose $l \in B$, then counting the occurrences of treatments of B in the remaining blocks of D_1, containing l and using Lemma 9 we have

$$(\lambda_1 - 1)t_l + (\lambda_2 - 1)(k - 1 - t_l) = (\lambda - 1)(r - 1)$$

since $\lambda_1 - \lambda_2 = q^{d-3} \neq 0$, solving the above equation for t_l, we get

$$t_l = (q + 1)q\left(\frac{q^{d-2} - 1}{q - 1}\right) \qquad \text{for} \quad l \in B.$$

Similarly, if $l \in B$, we can obtain the following equation

$$\lambda_1 t_l + \lambda_2(k - t_l) = \lambda r$$

and hence

$$t_l = q\left(\frac{q^{d-2} - 1}{q - 1}\right) + 1 = \frac{q^{d-1} - 1}{q - 1} \qquad \text{for } l \notin B.$$

Thus we have proved

Lemma 10 *For $l \in X$ and $B \in \mathcal{B}$, if t_l is as defined above, then t_l is independent of the choice of B and is given by*

$$t_l = (q + 1)q\left(\frac{q^{d-2} - 1}{q - 1}\right) \qquad \textit{for} \quad l \in B$$

$$\textit{and} \qquad t_l = \frac{q^{d-1} - 1}{q - 1} \qquad \textit{for} \quad l \notin B.$$

Lemma 11 *Let $d \geq 6$. There exists a unique BIBD $D_2 = (X_2, X, I_2)$ with parameters*

$$\left(\frac{q^{d+1} - 1}{q - 1}, \frac{(q^{d+1} - 1)(q^d - 1)}{(q^2 - 1)(q - 1)}, \frac{q^d - 1}{q - 1}, q + 1, 1\right), \qquad \textit{s.t. } G(D_2') \simeq G_1.$$

Proof Since $d \geq 6$, the conditions of Proposition 5 are satisfied for the graph G_1 and the result follows from the same.

From now on we shall assume that $d \geq 6$ and D_2 is the design defined by the above lemma. We note that blocks of D_2 are the treatments of D_1. We define a new incidence structure $D_3 = (X_2, \mathcal{B}, I_3)$ as follows. Treatments of D_2 are the treatments of D_3, while the blocks of D_1 are the blocks of D_3. A treatment x of D_3 is incident with the block B iff there exists $l \in X$ s.t. $x \in l$ in D_2 and $l \in B$ in D_1.

We proceed to compute the block size k_3 in D_3. Let B be a block of D_3. For each treatment $x \in B$ in D_3, define α_x to be the number of treatments l of D_1 s.t. $l \in B$ in D_1 and $x \in l$ in D_2. We first show that $\alpha_x = (q^{d-1} - 1) \mid q - 1$ for each $x \in B$ in D_3. Let l be any treatment of D_1 s.t. $l \in B$ in D_1. Then using Lemma 10 and the definition of D_2, etc., we have

$$\sum \alpha_x = (q+1)\left(q\left(\frac{q^{d-2}-1}{q-1}\right) + 1\right) \tag{3.4}$$

where the summation is over all the $q + 1$ treatments $x \in l$ in D_2.

Also if for each $x \in l$ in D_2 there is some treatment l' of D_1, $l' \notin B$ in D_1 s.t. $x \in l'$ in D_2, then again using Lemma 10, etc., we have

$$\alpha_x \leq t_{l'} = \frac{q^{d-1}-1}{q-1} = \frac{q(q^{d-2}-1)}{q-1} + 1. \tag{3.5}$$

Using (3.4) and (3.5) it follows that

$$\alpha_x = q\left(\frac{q^{d-2}-1}{q-1}\right) + 1 \qquad \text{for all} \quad x \in l$$

$$\text{or there is some } x \in l \text{ in } D_2 \text{ s.t. } \alpha_x = \frac{q^d - 1}{q-1}. \tag{3.6}$$

Suppose there exists $x \in B$ in D_3 s.t.

$$\alpha_x = \frac{q^d - 1}{q-1} \tag{3.7}$$

We next show that for all $z \neq x$, $z \in B$, $\alpha_z < q(q^{d-2} - 1)/(q - 1)$.

Now if z is any treatment of D_3, $z \in B$, $z \neq x$, then using (3.7), if l' is the unique block of D_2 containing x and z, $l' \in B$ in D_1. Hence using (3.4) for l' we have

$$\alpha_z \leq (q+1)q\left(\frac{q^{d-1}-1}{q-1}\right) - \frac{q^d - 1}{q-1} < q\left(\frac{q^{d-2}-1}{q-1}\right) \tag{3.8}$$

for all $z \in B$ in D_3, $z \neq x$.

Now since the block size in D_1 is $(q^d - 1)(q^{d-1} - 1)/(q^2 - 1)(q - 1)$, there is at least one treatment l' of D_1 s.t. $l' \in B$ in D_1 but $x \notin l'$ in D_2.

Equation (3.6) for l' and Eq. (3.8) give a contradiction. Hence

$$\alpha_x = q\left(\frac{q^{d-2}-1}{q-1}\right)+1 = \frac{q^{d-1}-1}{q-1} \tag{3.9}$$

for all $x \in B$ in D_3.

Now using (3.9), by counting the number of elements in the set $\{(x, l) \mid x \in l \text{ in } D_2, l \in B \text{ in } D_1\}$ we have

$$\left(\frac{q^{d-1}-1}{q-1}\right)k_3 = \frac{(q^d-1)(q^{d-1}-1)}{(q-1)(q^2-1)}(q+1).$$

Hence

$$k_3 = (q+1)\left(\frac{q^d-1}{q^2-1}\right) = \frac{q^d-1}{q-1} \tag{3.10}$$

for all blocks B of D_3. We can now prove the following lemma.

Lemma 12 *Let $d \geq 6$. Then D_3 is an SBIBD*

$$\left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}\right).$$

Proof It is obvious that the number of treatments or the number of blocks in D_3 is

$$v_3 = \frac{q^{d+1}-1}{q-1}.$$

Using (3.10) it follows that each block of D_3 is of size k_3, where

$$k_3 = \frac{q^d-1}{q-1}.$$

Hence we have only to prove that any two treatments of D_3 occur in exactly $(q^{d-1}-1)/(q-1)$ blocks. Suppose x_1 and x_2 are two treatments of D_3. Then there is a unique treatment l of D_1 s.t. $x_1, x_2 \in l$ in D_2. Now l occurs in exactly $r = (q^{d-1}-1)/(q-1)$ blocks of D_1. Hence x_1, x_2 occur in at least $(q^{d-1}-1)/(q-1)$ blocks of D_3. Counting the elements of the set

$$\{(y, z, B) \mid y, z \in X_2, y, z \in B \text{ in } D_3, B \in \mathscr{B}\},$$

we easily derive that in D_3 any two distinct treatments are incident with exactly $(q^d-1)/(q-1)$ blocks. This completes the proof.

We can now complete the proof of Theorem 1. We first note that the blocks of the BIBD D_2 correspond to the lines of D_3. For $l \in X$, let (l) denote the elements of X_2 incident with l in D_2. It is easily proved that for $x, y \in (l)$,

(l) is the line generated by x and y in D_3. For the sake of brevity, l will also denote the line of D_3. Using Lemma 10 given any block B of D_3 and a line l of D_3, there exists at least one treatment m of D_1 s.t. $m \in B$ and l and m are incident with a common block of D_1. Therefore any line and any block of D_3 intersect. Thus the conditions of Proposition 6 are satisfied. Hence $D_3 \simeq P_{0,d-1}(d, q)$. It follows that $D_1 \simeq P_{1,d-1}(d, q)$ and $G_1 \simeq G(P_{1,d-1})$ and q is a prime power.

4. Geometric Designs

In this section we shall study regular geometric designs. We shall also study geometric designs of rank 4. We shall first prove Theorem 2.

Let $D = (X, \mathcal{B}, I)$ be a regular geometric design of rank $d \geq 3$. Let $d \geq j \geq 3$. Let $P \subseteq X$ be any $(j-3)$-flat of D. And $Q \supseteq P$ be a j-flat of D. We define an incidence structure $D_{P,Q}$ as follows. Treatments of $D_{P,Q}$ are all $(j-2)$-flats that contain P and are contained in Q. Blocks are all $(j-1)$-flats that contain P and are contained in Q. Incidence is given by containment. The following result can be proved easily. In fact the usual proof for projective spaces can be extended to regular geometric designs [12].

Proposition 13 *$D_{P,Q}$ is a BIBD with parameters*

$$\left(\frac{m_j - m_{j-3}}{m_{j-2} - m_{j-3}}, \frac{(m_j - m_{j-3})(m_j - m_{j-2})}{(m_{j-1} - m_{j-3})(m_{j-1} - m_{j-2})}, \frac{m_j - m_{j-2}}{m_{j-1} - m_{j-2}}, \frac{m_{j-1} - m_{j-3}}{m_{j-2} - m_{j-3}}, 1\right)$$

Proof of Theorem 2 Let $D = (X, \mathcal{B}, I)$ be a regular geometric design as defined above. Using (1.2) and (1.3) for $D_{P,Q}$ we have

$$\frac{m_j - m_{j-2}}{m_{j-1} - m_{j-2}} \geq \frac{m_{j-1} - m_{j-3}}{m_{j-2} - m_{j-3}}.$$

Hence

$$\frac{m_j - m_{j-1}}{m_{j-1} - m_{j-2}} \geq \frac{m_{j-1} - m_{j-2}}{m_{j-2} - m_{j-3}} \quad \text{for all} \quad d \geq j \geq 3. \tag{4.1}$$

Using (4.1) it follows that

$$\frac{m_i - m_{i-1}}{m_{i-1} - m_{i-2}} \geq m_2 - 1 \quad \text{for all} \quad i \geq 3$$

hence $m_i - m_{i-1} \geq (m_2 - 1)(m_{i-1} - m_{i-2})$ for $d \geq i \geq 3$. This proves statement (a). Now suppose

$$m_i - m_{i-1} = (m_2 - 1)(m_{i-1} - m_{i-2}) \quad \text{for some } i.$$

Then we will have equality in (4.1) for all j, $i \geq j \geq 3$. In particular

$$m_3 - m_2 = (m_2 - 1)^2.$$

Hence

$$m_3 = (m_2 - 1)^2 + (m_2 - 1) + 1.$$

Thus if Q is a rank 3 flat of D and 0 denotes the 0-flat, then $D_{Q,0}$ will be a projective plane for all Q. Now let D_1 be an incidence structure defined as follows. Treatments of D_1 are the treatments of D. Blocks of D_1 are all the 3-flats of D. It is obvious that D_1 is a regular geometric design of rank 4. If $m_2 \geq 3$, then D_1 satisfies the conditions of Proposition 7 and hence $D_1 \simeq P_{0,2}(d, q)$ for some d and prime power q. Now it follows easily that $D \simeq P_{0,n}(d, q)$ and $d \geq n + 1$. If $m_2 = 2$, then any three points determine a unique 3-flat of D, and hence clearly they are incident with exactly

$$\frac{(m_n - m_3)(m_n - m_4) \cdots (m_n - m_{n-2})}{(m_{n-1} - m_3) \cdots (m_{n-1} - m_{n-2})}$$

blocks of D. Thus D is a 3-design. This completes the proof of the theorem. Theorem 3 is the obvious inductive extension of Theorem 2.

For the rest of this section we shall assume that $D = (X, \mathscr{B}, I)$ is a geometric design of rank 4. Let the parameters of D be (v, b, r, k, λ). Since rank $D = 4$, $\lambda > 1$.

Lemma 14 *All geometric design of rank* 4 *are regular.*

Proof Let D be a geometric design of rank 4, with parameters (v, b, r, k, λ). Let $x, y \in X$, $x \neq y$. Let l be the unique 2-flat containing x, y, i.e., line xy. Now from the properties of combinatorial geometries it follows that given $z \in X$, $z \notin l$, there is a unique block B of D s.t. $l \cup \{z\} \subseteq B$. Hence counting the number of elements in the set $\{(z, B) \mid z \in X - l, z \in B, l \subseteq B\}$, we have

$$\lambda(k - |l|) = v - |l|.$$

Hence

$$|l| = \frac{\lambda k - v}{\lambda - 1}.$$

Thus the cardinality of a line l is independent of the choice of the line l. Proof of Lemma 14 is now complete.

We now prove the final result of this paper.

Proof of Theorem 4 Using Lemma 14, D is a regular geometric design with

$$m_2 = \frac{\lambda k - v}{\lambda - 1} \quad \text{and} \quad m_3 = k. \tag{4.2}$$

Since m_2 is an integer, $v = k \bmod(\lambda - 1)$. Also since $m_2 \geq 2$,

$$\lambda k - v \geq 2(\lambda - 1).$$

Hence

$$v \leq \lambda k - 2(\lambda - 1).$$

Suppose $v = \lambda k - 2(\lambda - 1)$. Then $m_2 = 2$ and clearly D is a 3-$(v, k, 1)$-design. Thus we have proved (c). We now prove the remaining parts of Theorem 4. Using Theorem 2(a) for $i = 3$, we have

$$k \geq m_2(m_2 - 1) + 1. \tag{4.3}$$

Hence using (4.1) we have

$$v^2 - v(2\lambda k - (\lambda - 1)) + \lambda^2 k^2 - (\lambda - 1)^2 k \leq 0.$$

Hence

$$v \geq \lambda k - \frac{\lambda - 1}{2} - \frac{1}{2}\sqrt{(2\lambda k - (\lambda - 1))^2 + 4(\lambda^2 k^2 - (\lambda - 1)^2 k)}$$

i.e.,

$$v \geq \lambda k - \frac{\lambda - 1}{2} - \frac{\lambda - 1}{2}\sqrt{4k - 3}.$$

This proves (b). Now suppose $v = \lambda k - \frac{1}{2}(\lambda - 1) - \frac{1}{2}(\lambda - 1)\sqrt{4k - 3}$; then we will have equality in (4.3) and the statement (d) follows from Theorem 2(b).

Now suppose $v > \lambda k - \frac{1}{2}(\lambda - 1) - \frac{1}{2}(\lambda - 1)\sqrt{4k - 3}$. Hence

$$k > m_2(m_2 - 1) + 1.$$

Thus if P is any 3-flat of D and 0 denotes the 0-flat, then $D_{P,0}$ is not an SBIBD. Parameters of $D_{P,0}$ are

$$\left(m_3, \frac{m_3(m_3 - 1)}{m_2(m_2 - 1)}, \frac{m_3 - 1}{m_2 - 1}, m_2, 1\right).$$

Hence

$$\frac{m_3 - 1}{m_2 - 1} \geq m_2 + 1 \tag{4.4}$$

i.e., $k \geq m_2^2$. Hence using (4.2) we have

$$v^2 - 2\lambda k v - (\lambda - 1)^2 k + \lambda^2 k^2 \leq 0.$$

Hence

$$v \geq \lambda k - \tfrac{1}{2}\sqrt{4\lambda^2k^2 - 4[(\lambda - 1)^2k + \lambda^2k^2]}$$

i.e.,

$$v \geq \lambda k - (\lambda - 1)\sqrt{k}.$$

If $v = \lambda k - (\lambda - 1)\sqrt{k}$ and $k \geq 16$, then we will have equality in (4.4) and $m_2 \geq 4$. Hence all designs $D_{P,0}$ are affine planes, and the statement (e) follows from Proposition 8. This completes the proof of the theorem.

A natural question arises. Are there geometric designs of rank 4 different from those given by cases (c)–(e) of Theorem 4. We note that using examples of Steiner triple systems due to Hall [6], one can construct one such geometric designs of rank 4 (see also Teirlinck [11]). This example also shows that the hypothesis $k \geq 16$ in statement (e) is necessary. An interesting problem will be to classify all geometric designs of rank 4.

REFERENCES

[1] F. Beukenhout, Cáracterisation des espaces affine basée sur la notion de droit, *Math. Z.* **3** (1969), 367–371.

[2] R. C. Bose, Strongly regular graphs, partial geometries and partially balanced designs, *Pacific J. Math.* **13** (1963), 389–419.

[3] H. H. Crapo and G.-C. Rota, "Combinatorial Geometries." MIT Press, Cambridge, Massachusetts, 1970.

[4] P. Dembowski, "Finite Geometries." Springer-Verlag, Berlin and New York, 1968.

[5] P. Dembowski and A. Wagner, Some characterizations of finite projective spaces, *Arch. Math. (Basel)* **11** (1960), 465–469.

[6] M. Hall, Automorphisms of Steiner triple systems, *Proc. Symposia Pure Math.* **VI,** Amer. Math. Soc., Providence, Rhode Island, 1962.

[7] W. M. Kantor, Characterizations of finite projective and affine spaces, *Canad. J. Math.* **21** (1969), 64–75.

[8] V. C. Mavron, On the structure of affine designs, *Math. Z.* **125** (1972), 298–316.

[9] D. K. Ray-Chaudhuri and A. P. Sprague, Characterization of projective incidence structures, *Geometriae Dedicata*, to appear.

[10] D. K. Ray-Chaudhuri, "Uniqueness of Association Schemes." Proc. Int. Coll. Combinatorial Theory, Acad. Lincei, Rome, 1973.

[11] L. Teirlinck, On linear spaces in which every plane is projective or affine, *Geometriae Dedicata* **4** (1975), 39–44.

[12] P. Young, U. S. R. Murti, and J. Edmonds, Equicardinal matroids and matroid designs, "Proceedings of the Second Chapel Hill Conference," 498–547. Univ. of North Carolina Press, Chapel Hill, North Carolina, 1970.

On the Behavior of Ideal Classes in Cyclic Unramified Extensions of Prime Degree

ROSS SCHIPPER†

DEPARTMENT OF DEFENSE
WASHINGTON, D.C.

If K/F is a cyclic unramified extension of number fields of prime degree p and $\Psi_{F\to K}$: $\mathrm{Cl}(F)\to \mathrm{Cl}(K)$ is the ideal class mapping, then $\#(\mathrm{Ker}(\Psi_{F\to K}))$ is bounded above by p^{r+w-1} where r is the rank of E_F as a $\mathbf{Z}$-module, $w=1$ if F contains the pth roots of unity, and $w=0$ otherwise. Noticing that this bound goes to infinity along with $[K:\mathbf{Q}]$, we ask the question, Can one construct a sequence of extensions K/F for which $\#(\mathrm{Ker}(\Psi_{F\to K}))$ goes to infinity along with $[K:\mathbf{Q}]$? This question is settled by the following theorem which we prove here:

Let L be any number field and p a fixed rational prime. Then there exists a cyclic extension F of degree p over L which in turn possesses a cyclic unramified extension K of degree p over F satisfying p^r divides $\#(H^1(\mathrm{Gal}(K/F), E_K))$ where r is the rank of E_L as a $\mathbf{Z}$-module.

1. Introduction

Let F be a number field and K a finite Galois extension of F. The extension K/F is said to be unramified if no prime of F (finite or infinite) ramifies in K/F. If $\mathfrak{A}$ is a nonprincipal ideal of F, then we say that $\mathfrak{A}$ capitulates in K/F if the K-ideal $\mathfrak{A}\mathfrak{O}_K$ is principal. There is a natural homomorphism $\Psi_{F\to K}$: $\mathrm{Cl}(F)\to \mathrm{Cl}(K)$ given by $\mathrm{Cl}(\mathfrak{A})\mapsto \mathrm{Cl}(\mathfrak{A}\mathfrak{O}_K)$, where $\mathrm{Cl}(F)$

† Present address: 6300 Golden Hook, Columbia, Maryland.

denotes the ideal class group of F and $\mathrm{Cl}(\mathfrak{A})$ denotes the ideal class to which $\mathfrak{A}$ belongs. Thus $\mathfrak{A}$ capitulates in K/F if and only if $\mathrm{Cl}(\mathfrak{A})$ belongs to $\mathrm{Ker}(\Psi_{F\to K})$. When this occurs, we also say that $\mathrm{Cl}(\mathfrak{A})$ capitulates. As long as K and F are understood, we shall write Ψ instead of $\Psi_{F\to K}$.

There are two basic tools for analyzing $\mathrm{Ker}(\Psi)$. The first concerns a group theoretic homomorphism called the transfer. The second, and the one we shall use, is the following theorem due to Iwasawa [2]:

Theorem 1 *Let K/F be an unramified Galois extension of number fields with Galois group G, and let E_K denote the group of units of K. Then* $\mathrm{Ker}(\Psi) \simeq H^1(G, E_K)$.

Now let K/F be a cyclic unramified extension of prime degree p. There is a natural lower bound on $\#(\mathrm{Ker}(\Psi))$, namely for such an extension, p divides $\#(\mathrm{Ker}(\Psi))$. This result is known as Hilbert's theorem 94 and follows from Theorem 1 and the well-known fact that

$$\#(H^0(G, E_K))/\#(H^1(G, E_K)) = [K : F]^{-1}$$

(see for instance Lang [3, p. 192]). There is also a natural upper bound on $\#(\mathrm{Ker}(\Psi))$.

Lemma 2 $\#(\mathrm{Ker}(\Psi))$ *divides* p^{r+w+1} *where r is the rank of E_F as a* $\mathbf{Z}$*-module, $w = 1$ if F contains the* pth *roots of* 1, *and $w = 0$ otherwise.*

Proof By Theorem 1, $\mathrm{Ker}(\Psi) \simeq H^1(G, E_K)$ where $G = \mathrm{Gal}(K/F)$. Also by the Herbrand quotient, $\#(H^1(G, E_K)) = p\ \#(H^0(G, E_K))$. Now $H^0(G, E_K) = E_F/N_{K/F}(E_K)$ and $E_F^p \subseteq N_{K/F}(E_K)$. Moreover, as a $\mathbf{Z}$-module, $E_F \simeq W \oplus \mathbf{Z}^r$ where W is the cyclic group of roots of unity of F. Thus E_F/E_F^p has order p^{r+w} where $w = 1$ if p divides $\#(W)$ and $w = 0$ otherwise. Thus $\#(H^0(G, E_K))$ divides p^{r+w} so that $\#(\mathrm{Ker}(\Psi))$ divides p^{r+w+1}. ∎

Now r is equal to $r_1 + r_2 - 1$ where r_1 is the number of real embeddings of F into $\mathbf{C}$ and r_2 is the number of conjugate pairs of complex embeddings of F into $\mathbf{C}$. Thus we see that the upper bound of Lemma 2 goes to infinity along with $[F : \mathbf{Q}]$. If $N: \mathrm{Cl}(K) \to \mathrm{Cl}(F)$ denotes the homomorphism induced by the norm of ideals, then

$$N(\Psi(\mathrm{Cl}(\mathfrak{A}))) = \mathrm{Cl}(\mathfrak{A})^p$$

so that $\mathrm{Ker}(\Psi)$ is an elementary abelian p-group. Let t be its dimension as a vector space over $\mathbf{Z}/p\mathbf{Z}$. We consider the following question. Can we find cyclic unramified extensions K/F of prime degree p for which t is as large as we wish? That the answer to this question is yes follows from Theorem 1 and the next theorem whose proof will absorb the remainder of this paper.

Theorem 3 *Let L be any number field and p a fixed rational prime. Then there exists a cyclic extension F of degree p over L which in turn possesses a cyclic unramified extension K of degree p over F satisfying:*

$$p^r \quad \textit{divides } \#(H^1(\mathrm{Gal}(K/F), E_K))$$

where r is the rank of E_L as a $\mathbf{Z}$-module.

2. Proof of Theorem 3

We will assume throughout that L is neither $\mathbf{Q}$ nor any imaginary quadratic field since in these cases $r = 0$ and the theorem is trivial. To prove the theorem, we shall construct a cyclic extension K_1 of L of degree p for which

$$N_{K_1/L}(E_{K_1}) = E_L^p \tag{1}$$

and

$$\begin{aligned} &K_1/L \text{ is unramified at the infinite primes} \\ &\text{of } L \text{ and there exists a finite prime of} \\ &L \text{ ramified in } K_1/L. \end{aligned} \tag{2}$$

Then we shall construct another cyclic extension K_2 of L of degree p such that

$$\begin{aligned} &\text{If } \mathfrak{p} \text{ is a finite prime of } L \text{ ramified in} \\ &K_1/L, \text{ then } \mathfrak{p} \text{ is unramified in } K_2/L \end{aligned} \tag{3}$$

and

$$\begin{aligned} &\text{The compositum } K = K_1K_2 \text{ is such that} \\ &N_{K/K_1}(E_K) = E_{K_1}^p. \end{aligned} \tag{4}$$

Before actually constructing K_1 and K_2, let us show that their existence suffices to prove the theorem.

First, K_1 and K_2 are linearly disjoint over L. For there exists a prime $\mathfrak{p}$ of L ramified in K_1/L and such a $\mathfrak{p}$ is unramified in K_2/L. Thus $\mathrm{Gal}(K/L) \simeq \mathbf{Z}/p\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}$ and so there exists a subfield F of K containing L with F distinct from K_1 and K_2 and with $[K : F] = [F : L] = p$. Choose any such F. We shall show that K/F satisfies the conclusions of the theorem.

It is easy to see that K/F is unramified, for suppose $\mathfrak{P}$ is a finite prime of F ramified in K/F. If $\mathfrak{p}$ is the L-prime that $\mathfrak{P}$ divides, then $\mathfrak{p}$ ramifies in K_1/L and in K_2/L, which is impossible by the construction of K_2. Moreover, the infinite primes of F are unramified in K/F since the infinite primes of L are unramified in K_1/L.

It remains to show that p^r divides $\#(H^1(G, E_K))$ where $G = \mathrm{Gal}(K/F)$. Let W_K denote the group of roots of unity of K. By (1) and (4), $N_{K/L}(E_K) = E_L^{p^2}$. It then follows that

$$E_K/W_K \simeq E_L W_K/W_K \oplus ({}_{N_{K/L}}(E_K))W_K/W_K$$

where ${}_{N_{K/L}}(E_K)$ is the group of units η of K for which $N_{K/L}(\eta) = 1$ and the direct sum is as $\mathbf{Z}[G]$-modules. For if $\xi \in E_K$, then $N_{K/L}(\xi) = \eta^{p^2}$ where $\eta \in E_L$ is unique modulo roots of unity and $\xi\eta^{-1} \in {}_{N_{K/L}}(E_K)$. Thus

$$H^0(G, E_K/W_K) \simeq H^0(G, E_L W_K/W_K) \oplus H^0(G, ({}_{N_{K/L}}(E_K))W_K/W_K).$$

We cannot say much about the second factor in this direct sum decomposition, but since G acts trivially on $E_L W_K/W_K$ and $E_L W_K/W_K$ is a free $\mathbf{Z}$-module of rank r, $\#(H^0(G, E_L W_K/W_K)) = p^r$ and thus we see that p^r divides $\#(H^0(G, E_K/W_K))$. Then by the Herbrand quotient, p^{r+1} divides $\#(H^1(G, E_K/W_K))$. Now from the exact sequence of G-modules,

$$1 \longrightarrow W_K \longrightarrow E_K \xrightarrow{\pi} E_K/W_K \longrightarrow 1,$$

we obtain an exact sequence of cohomology groups,

$$\longrightarrow H^1(G, W_K) \longrightarrow H^1(G, E_K) \xrightarrow{\pi^*} H^1(G, E_K/W_K) \xrightarrow{\delta} H^0(G, W_K) \longrightarrow.$$

But $\#(H^0(G, W_K))$ divides $\#(W_K/W_K^p) = p^w$ where $w = 1$ if K contains the pth roots of 1 and $w = 0$ otherwise. Hence the order of $\mathrm{Im}(\pi^*) = \mathrm{Ker}(\delta)$ is divisible by p^{r+1-w} so that p^r divides $\#(H^1(G, E_K))$.

3. Construction of K_1 and K_2

To complete the proof, we must construct K_1 and K_2. We shall construct K_1 first.

Let $1, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_s$ denote a system of coset representatives of E_L/E_L^p. Let $L_1 = L(\zeta_p)$ where ζ_p is a primitive pth root of unity. Let us first observe that an element $\alpha \in L$ belongs to $(L^\times)^p$ if and only if $\alpha \in (L_1^\times)^p$. This is obvious since $[L_1 : L]$ is prime to p. For each i, let $M_i = L_1(\varepsilon_i^{1/p})$ where $\varepsilon_i^{1/p}$ denotes a root of $x^p - \varepsilon_i$ in $\mathbf{C}$. By our observation above and our choice of ε_i, we see that $[M_i : L_1] = p$. Since M_i/L_1 is cyclic, the density of primes of L_1 that split completely in M_i is $1/p < 1$. Thus there exist infinitely many L_1-primes that do not split completely in M_i. Now choose distinct L_1-primes $\mathfrak{P}_i$ that are to satisfy:

1. $\mathfrak{P}_i$ does not split completely in M_i; and
2. $\mathfrak{P}_i$ does not divide $2\mathfrak{O}_{L_1}$.

Let $\mathfrak{p}_i$ denote the L-prime that $\mathfrak{P}_i$ divides.

Suppose $\varepsilon_i = \beta_i^p$ for some $\beta_i \in L_{1,\mathfrak{P}_i}^{\times}$, then $L_{1,\mathfrak{P}_i}(\varepsilon_i^{1/p}) = L_{1,\mathfrak{P}_i}$ so that $\mathfrak{P}_i$ splits completely in M_i/L_1 contrary to the choice of $\mathfrak{P}_i$. We conclude that $\varepsilon_i \notin (L_{1,\mathfrak{P}_i}^{\times})^p$. All the more so, $\varepsilon_i \notin (L_{\mathfrak{p}_i}^{\times})^p$. Moreover, $\mathfrak{p}_i$ does not divide $2\mathfrak{O}_L$.

Now $L_{\mathfrak{p}_i}^{\times}/(L_{\mathfrak{p}_i}^{\times})^p$ is a finite elementary abelian p-group. Since $\varepsilon_i \notin (L_{\mathfrak{p}_i}^{\times})^p$, we can choose a subgroup H_i of $L_{\mathfrak{p}_i}^{\times}$ of index p not containing ε_i. By local class field theory, there exists a cyclic extension F_i of degree p over $L_{\mathfrak{p}_i}$ with $N_{F_i/L_{\mathfrak{p}}}(F_i^{\times}) = H_i$. Note that $\varepsilon_i \in U_{\mathfrak{p}_i}$, the unit group of $L_{\mathfrak{p}_i}$, so that $U_{\mathfrak{p}_i} \not\subseteq H_i$ and hence $F_i/L_{\mathfrak{p}_i}$ is ramified. Let $\chi_{\mathfrak{p}_i}\colon L_{\mathfrak{p}_i}^{\times} \to T$ be a continuous local character with $\mathrm{Ker}(\chi_{\mathfrak{p}_i}) = H_i$ where here T denotes the set of complex numbers of absolute value 1. If S_∞ denotes the set of real infinite primes of L, then for each $\mathfrak{p}_\infty \in S_\infty$, let $\chi_{\mathfrak{p}_\infty}\colon R \to T$ be the trivial character. Now set $S = \{\mathfrak{p}_i\colon 1 \leq i \leq s\} \cup S_\infty$ and apply a variant of Grumwald's existence theorem [1, p. 103, Theorem 5]. Since no $\mathfrak{p}_i$ divides $2\mathfrak{O}_L$, $S_0 \not\subseteq S$ where $S_0 = \{\mathfrak{p} \mid \mathfrak{p} \text{ divides } 2\mathfrak{O}_L\}$. Thus there exists a continuous global character $\chi\colon C_L \to T$ of order p (the $\chi_{\mathfrak{p}_i}$ have order p and the $\chi_{\mathfrak{p}_\infty}$ have order 1) whose restriction to $L_{\mathfrak{p}}^{\times}$ is $\chi_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$ (here C_L denotes the idèle class group of L and we view $L_{\mathfrak{p}_i}^{\times}$ embedded in C_L in the usual manner). Let $M = \mathrm{Ker}(\chi)$. Since χ is continuous and T Hausdorff, $\mathrm{Ker}(\chi)$ is closed. Moreover, $[C_L : M] = p$ since χ has order p and $\mathrm{Im}(\chi) \subseteq T$ is cyclic. Thus M is an open subgroup of C_L of finite index p. By class field theory, there exists a cyclic extension K_1 of L of degree p such that $N_{K_1/L}(C_{K_1}) = M$.

We shall now show that K_1 has the desired properties. If P_i is a prime of K_1 dividing $\mathfrak{p}_i\mathfrak{O}_{K_1}$, then

$$N_{K_{1,P_i}L_{\mathfrak{p}_i}}(K_{1,P_i}^{\times}) = M \cap L_{\mathfrak{p}_i}^{\times} = \mathrm{Ker}(\chi) \cap L_{\mathfrak{p}_i}^{\times}$$
$$= \mathrm{Ker}(\chi|_{L_{\mathfrak{p}_i}}^{\times}) = \mathrm{Ker}(\chi_{\mathfrak{p}_i}) = H_i,$$

and so $\varepsilon_i \notin N_{K_{1,P_i}/L_{\mathfrak{p}_i}}(K_{1,P_i}^{\times})$. Thus $\varepsilon_i \notin N_{K_1/L}(K_1^{\times})$ for $1 \leq i \leq s$ and (1) follows. Also, if $\mathfrak{p}_\infty \in S_\infty$, then $N_{K_{1,\mathfrak{P}_\infty}/L_{\mathfrak{p}_\infty}}(K_{1,\mathfrak{P}_\infty}^{\times}) = L_{\mathfrak{p}_\infty}^{\times}$ so that $\mathfrak{p}_\infty$ is unramified in K_1/L. In addition, by our original assumption on L, $s \geq 1$ and so, as we observed during the construction, some finite prime of L ramifies in K_1/L. Thus (2) is also satisfied.

The construction of K_2 is similar to that of K_1 and we will leave out some details at the points of similarity.

Let $1, \eta_1, \eta_2, \ldots, \eta_t$ denote a system of coset representatives of $E_{K_1}/E_{K_1}^p$. For each i, let $K_{1,i} = K_1(\eta_i^{1/p})$ where $\eta_i^{1/p}$ denotes a fixed root of $x^p - \eta_i$ in $\mathbf{C}$. Choose distinct L-primes $\mathfrak{q}_i$ which are to satisfy:

1. $\mathfrak{q}_i$ splits completely in K_1/L;
2. $\mathfrak{q}_i$ does not divide $2\mathfrak{O}_L$; and
3. if $\mathfrak{Q}_i$ is a K_1-prime over $\mathfrak{q}_i$, then $\eta_i \notin (K_{1,\mathfrak{Q}_i}^{\times})^p$.

To see that such q_i exist, we first notice that there exist infinitely many L-primes that split completely in $K_1(\zeta_p)/L$ but do not split completely in $K_{1,i}(\zeta_p)/L$. Then by an argument similar to the one used in the construction of K_1, we see that properties 1 and 3 are satisfied for such a q_i. See Fig. 1.

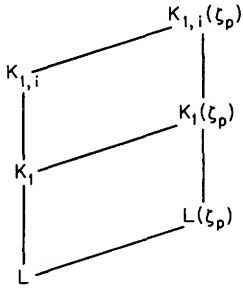


FIG. 1

Since q_i splits completely in K_1/L, $K_{1,\mathfrak{Q}_i} = L_{q_i}$ and by 3, $\eta_i \notin (L_{q_i}^{\times})^p$. Again, there exists a cyclic local extension M_i/L_{q_i} of prime degree p for which $\eta_i \notin N_{M_i/L_{q_i}}(M_i^{\times})$. Set

$$A = \{L\text{-primes } \mathfrak{p} : \mathfrak{p} \text{ ramifies in } K_1/L\},$$

$$S_0 = \{L\text{-primes } \mathfrak{p} : \mathfrak{p} \text{ divides } 2\mathfrak{O}_L\},$$

$$S = \{q_i : 1 \le i \le t\} \cup S_0 \cup A.$$

As before, define continuous local characters $\chi_{q_i}: L_{q_i}^{\times} \to T$ with $\mathrm{Ker}(\chi_{q_i}) = N_{M_i/L_{q_i}}(M_i^{\times})$. In addition, for each $\mathfrak{p} \in A \cup S_0$, let $\chi_{\mathfrak{p}}: L_{\mathfrak{p}}^{\times} \to T$ be the trivial character. Since $\prod_{\mathfrak{p} \in S_0} \chi_{\mathfrak{p}} \equiv 1$, there exists a continuous global character $\chi: C_L \to T$ of order p for which $\chi|_{L_{\mathfrak{p}}} = \chi_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$ (again see Artin and Tate [1, p. 103, Theorem 5]). Let K_2 be the cyclic extension of L of degree p determined by χ. It remains to show that K_2 satisfies the desired properties.

Let $\mathfrak{Q}_i$ be a prime of K_1 over q_i, let $\mathfrak{P}_i'$ be a prime of $K = K_1 K_2$ over $\mathfrak{Q}_i$, and let $\mathfrak{p}_i'$ be the prime of K_2 that $\mathfrak{P}_i'$ divides. By construction of K_2, $\eta_i \notin N_{K_{2,\mathfrak{p}_i'}/L_{q_i}}(K_{2,\mathfrak{p}_i'}^{\times})$. But q_i splits completely in K_1/L and so $\mathfrak{p}_i'$ splits completely in K/K_2. Hence $L_{q_i} = K_{1,\mathfrak{Q}_i}$ and $K_{2,\mathfrak{p}_i'} = K_{\mathfrak{P}_i'}$ and we see that $\eta_i \notin N_{K_{\mathfrak{P}'}/K_{1,\mathfrak{Q}}}(K_{\mathfrak{P}_i'}^{\times})$ for $1 \le i \le t$. It follows that $N_{K/K_1}(E_K) = E_{K_1}^p$ and so (4) is satisfied. Let $\mathfrak{p} \in A \cup S_0$. If $\mathfrak{P}$ is a K_2-prime above $\mathfrak{p}$, then $N_{K_{2,\mathfrak{P}}/L_{\mathfrak{p}}}(K_{2,\mathfrak{P}}^{\times}) = \mathrm{Ker}(\chi) \cap L_{\mathfrak{p}}^{\times} = \mathrm{Ker}(\chi|_{L_{\mathfrak{p}}}^{\times}) = L_{\mathfrak{p}}^{\times}$ so that $L_{\mathfrak{p}} = K_{2,\mathfrak{P}}$ and $\mathfrak{p}$ splits completely in K_2/L. In particular, $\mathfrak{p}$ is unramified in K_2/L. Thus (3) is also satisfied. This completes the proof of Theorem 3. ∎

REFERENCES

[1] E. Artin and J. Tate, "Class Field Theory." Benjamin, New York, 1967.
[2] K. Iwasawa, A note on the group of units of an algebraic number field, *J. Math. Pures Appl.* **35** (1956), 189–192.
[3] S. Lang, "Algebraic Number Theory." Addison-Wesley, Reading, Massachusetts, 1970.

Irregularities of Distribution, X†

WOLFGANG M. SCHMIDT

UNIVERSITY OF COLORADO ‡ AND UNIVERSITÄT WIEN
BOULDER, COLORADO VIENNA, AUSTRIA

1. Introduction

Suppose we are given N points in U^k, where $k > 1$ and U^k is the unit cube, consisting of points $\mathbf{y} = (y_1, \ldots, y_k)$ with $0 \leq y_i < 1$ $(i = 1, \ldots, k)$. For $\mathbf{x}$ in U^k, write $Z(\mathbf{x})$ for the number of points among the N given points that lie in the box $0 \leq y_i < x_i$ $(i = 1, \ldots, k)$, and put

$$D(\mathbf{x}) = Z(\mathbf{x}) - Nx_1 \cdots x_k .$$

The irregularity of the distribution of the given N points may be measured in various ways by the behavior of the function $D(\mathbf{x})$. For example, one may consider the L^p-norms

$$\| D \|_p = \left(\int | D(\mathbf{x}) |^p \, d\mathbf{x} \right)^{1/p} .$$

(Here and throughout, except where noted, the integrals are over U^k.) Roth

† Written with partial support from NSF-MCS 75-08233 A01.
‡ Present address.

[4] proved that for some $c_1(k) > 0$,

$$\| D \|_2 > c_1(k)(\log N)^{(k-1)/2}, \tag{1.1}$$

and Davenport [2] showed that for $k = 2$ this is best possible, except for the value of the constant $c_1(2)$.

Theorem 1 *For $p > 1$ there is a constant $c_1(k, p) > 0$ such that*

$$\| D \|_p > c_1(k, p)(\log N)^{(k-1)/2}. \tag{1.2}$$

Since $\| D \|_p$ cannot decrease with p, this estimate for $1 < p < 2$ is a sharpening of (1.1). Moreover, it is best possible for $k = 2$ and $1 < p \leq 2$. Perhaps it is best possible, except for the value of $c_1(k, p)$, for every $k > 1$, $p > 1$. We cannot give an estimate of the same strength for $\| D \|_1$. But with

$$E(\mathbf{x}) = D(\mathbf{x})(\log N)^{-(k-1)/2},$$

we have

Theorem 2 *For $q > k - \frac{3}{2}$, there is a $c_2 = c_2(k, q) > 0$ such that*

$$\int |c_2 E(\mathbf{x})| \, |\log |c_2 E(\mathbf{x})| \, |^q \, d\mathbf{x} > 1. \tag{1.3}$$

This contains Theorem 1: For pick $c_3 = c_3(q) > 0$ so small that $z |\log z|^q < \frac{1}{2}$ for $0 < z < c_3$. Then the integral of $|c_2 E(\mathbf{x})| \, |\log |c_2 E(\mathbf{x})| \, |^q$ over points $\mathbf{x}$ with $|c_2 E(\mathbf{x})| \geq c_3$ is $> \frac{1}{2}$. But in this domain $|c_2 E(\mathbf{x})|^p \geq c_4 \, |c_2 E(\mathbf{x})| \, |\log |c_2 E(\mathbf{x})| \, |^q$, where $c_4 > 0$ is the minimum of $z^{p-1} |\log z|^{-q}$ for z with $z \geq c_3$. Thus

$$\int |c_2 E(\mathbf{x})|^p \, d\mathbf{x} > \tfrac{1}{2} c_4 ,$$

and (1.2) follows.

Sobol [6] noted that

$$\| D \|_1 > \frac{1}{4} - \frac{c_5(k)}{N},$$

and in [3, 6] there is the statement that one can always give examples where $\|D\|_1 < \frac{1}{4}$. But Sobol gives such an example only for $N = 1$! In fact, we have

Theorem 3 *For some $c_6 = c_6(k) > 0$ and for large N (say $N > e^{100}$),*

$$\| D \|_1 > c_6 \log \log N / \log \log \log N.$$

The function on the right-hand side is the same as the one given by Aardenne-Ehrenfest [1] in her estimate of $\| D \|_\infty$, i.e., the supremum of $|D(\mathbf{x})|$. As far as I can see, this is a coincidence. It is possible that our

estimate of $\| D \|_1$ could be somewhat improved at the cost of a further complication of the proof.

For the sake of completeness we mention that at present the best estimates for $\| D \|_\infty$ are $\| D \|_\infty > c_1(k)(\log N)^{(k-1)/2}$ as a consequence of (1.1), and $\| D \|_\infty > c_7 \log N$ for $k = 2$, according to [5].

The following question is open: Is there a function $f(N)$, decreasing to 0, such that for any $C > 0$ the measure of the set of $\mathbf{x}$ with $|D(\mathbf{x})| < C$, is $O(f(N))$?

2. The Method

Roth obtained his estimate by constructing an auxiliary function $F(\mathbf{x})$ with

$$\int F(\mathbf{x})D(\mathbf{x})\, d\mathbf{x} > c_8(k)(\log N)^{k-1} \tag{2.1}$$

(where $c_8(k)$ as well as all of our constants are positive) and

$$\int F^2(\mathbf{x})\, d\mathbf{x} < c_9(k)(\log N)^{k-1}. \tag{2.2}$$

These two inequalities, together with Schwarz' inequality, yield (1.1). It may be shown that the very same function $F(\mathbf{x})$ also has

$$\int F^{2m}(\mathbf{x})\, d\mathbf{x} < c_9(k, m)(\log N)^{m(k-1)} \qquad (m = 1, 2, \ldots). \tag{2.3}$$

This is rather surprising since $F(\mathbf{x})$ was constructed with only (2.1) and (2.2) in mind. Now by (2.3),

$$\| F \|_{2m} < c_{10}(k, m)(\log N)^{(k-1)/2} \qquad (m = 1, 2, \ldots),$$

and since $\| F \|_r$ cannot decrease as a function of r, we have

$$\| F \|_r < c_{11}(k, r)(\log N)^{(k-1)/2} \qquad (r > 0). \tag{2.4}$$

Hölder's inequality yields

$$\int F(\mathbf{x})D(\mathbf{x})\, d\mathbf{x} \leq \| F \|_r \| D \|_p,$$

provided $p > 1$, $r > 1$ with $(1/p) + (1/r) = 1$. This inequality, together with (2.1), (2.4), gives (1.2).

We shall use a slightly modified function $F(\mathbf{x})$ with (2.1) and with

$$\int F^{2m}(\mathbf{x})\, d\mathbf{x} < (2m)^{m(2k-3)}(v + 1)^{m(k-1)} \qquad (m = 1, 2, \ldots), \tag{2.5}$$

where v is the integer determined by

$$2N \le 2^v < 4N. \tag{2.6}$$

This explicit estimate will be needed for Theorem 2. (Roth's function $F(\mathbf{x})$ would give (2.5) with the exponent $m(2k-3)$ replaced by $m(2k-2)$, which would yield (1.3) under the slightly more restrictive condition that $q > k-1$.)

In order to prove the more difficult Theorem 3, we shall need certain finite sums, rather than integrals over U^k. For Theorems 1 and 2, we could also have used finite sums, which perhaps would have made the exposition more uniform. But the notation with integrals is slightly simpler, and by using integrals we stay closer to the established style, as presented by Kuipers and Niederreiter [3] or Roth [4].

3. Generalized Rademacher Functions

Every x in $0 \le x < 1$ may uniquely be written as

$$x = \sum_{j=1}^{\infty} \beta_j(x) 2^{-j}$$

where the digits $\beta_j(x)$ are 0 or 1, and where the sequence of digits does not end with 1, 1, ... The functions

$$R_r(x) = (-1)^{\beta_{r+1}(x)} \qquad (r = 0, 1, \ldots)$$

are the Rademacher functions. (This notation is more convenient for us than the more common $R_r(x) = (-1)^{\beta_r(x)}$.)

An *r-interval* will be an interval

$$m2^{-r} \le x < (m+1)2^{-r},$$

where m is an integer in $0 \le m < 2^r$. An *r-function*, where r is a nonnegative integer, is defined as a function $f(x)$ in $0 \le x < 1$ such that in every r-interval, either $f(x) = R_r(x)$ or $f(x) = -R_r(x)$. There are 2^r r-intervals, hence 2^{2^r} r-functions. An r-function has

$$\int_0^1 f(x)\, dx = 0.$$

Lemma 1 *Suppose $f_1, \ldots, f_l$ are $r_1, \ldots, r_l$-functions, respectively. Suppose an odd number among $r_1, \ldots, r_l$ is equal to their maximum $r = \max(r_1, \ldots, r_l)$.*

Then the product $f_1(x)\cdots f_l(x)$ *is an r-function, and*

$$\int_0^1 f_1(x)\cdots f_l(x)\,dx = 0.$$

Proof It suffices to observe that the product of an odd number of r-functions is an r-function, and the product of an r-function and an s-function with $s < r$ is an r-function.

Given a k-tuple $\mathbf{r} = (r_1, \ldots, r_k)$ of nonnegative integers, put

$$|\mathbf{r}| = r_1 + \cdots + r_k. \tag{3.1}$$

For $\mathbf{x}$ in U^k, write

$$R_{\mathbf{r}}(\mathbf{x}) = R_{r_1}(x_1)\cdots R_{r_k}(x_k).$$

An $\mathbf{r}$-box is defined as a box $B = I_1 \times \cdots \times I_k$, where I_j is an r_j-interval for $j = 1, \ldots, k$. An $\mathbf{r}$-function is a function $f(\mathbf{x})$ on U^k such that in every $\mathbf{r}$-box either $f(\mathbf{x}) = R_{\mathbf{r}}(\mathbf{x})$ or $f(\mathbf{x}) = -R_{\mathbf{r}}(\mathbf{x})$. There are $2^{2^{|\mathbf{r}|}}$ such $\mathbf{r}$-functions. For given $x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_k$, an $\mathbf{r}$-function is an r_j-function in the variable x_j. Combining this remark with Lemma 1, we obtain

Lemma 2 *Suppose* $f_1, \ldots, f_l$ *are, respectively,* $\mathbf{r}_1, \ldots, \mathbf{r}_l$*-functions. Write* $\mathbf{r}_i = (r_{i1}, \ldots, r_{ik})$ *and* $r = \max(r_{1k}, \ldots, r_{lk})$*. Suppose an odd number among* $r_{1k}, \ldots, r_{lk}$ *equals* r*. Then*

$$\int f_1(\mathbf{x})\cdots f_l(\mathbf{x})\,d\mathbf{x} = 0.$$

In the lemma the kth coordinate is singled out. The same result is of course true for the jth coordinate with $1 \le j \le k$.

Lemma 3 *Suppose* $k = 2$, $v \ge 0$. *Suppose for each* $\mathbf{r}$ *with* $|\mathbf{r}| = v$ *we have picked an* $\mathbf{r}$*-function* $f_{\mathbf{r}}$. *For* $\mathbf{r}_1, \ldots, \mathbf{r}_{2m}$ *with* $|\mathbf{r}_1| = \cdots = |\mathbf{r}_{2m}| = v$*, put*

$$\mathfrak{I}(\mathbf{r}_1, \ldots, \mathbf{r}_{2m}) = \int f_{\mathbf{r}_1}(\mathbf{x})\cdots f_{\mathbf{r}_{2m}}(\mathbf{x})\,d\mathbf{x}. \tag{3.2}$$

Then $\mathfrak{I}(\mathbf{r}_1, \ldots, \mathbf{r}_{2m}) = 0$*, unless there is a decomposition of* $\{1, \ldots, 2m\}$ *into* m *pairs* $(i_1, j_1), \ldots, (i_m, j_m)$ *with* $\mathbf{r}_{i_t} = \mathbf{r}_{j_t}$ *for* $t = 1, \ldots, m$.

Proof For $m = 1$ we know from Lemma 2 that $\mathfrak{I}(\mathbf{r}_1, \mathbf{r}_2) = 0$ unless $r_{12} = r_{22}$, i.e., unless $\mathbf{r}_1 = \mathbf{r}_2$ in view of $|\mathbf{r}_1| = |\mathbf{r}_2|$. For $m > 1$, we know again that the integral is 0 unless $\mathbf{r}_{i_1} = \mathbf{r}_{j_1}$ for some $i_1 \neq j_1$. Since the square of an $\mathbf{r}$-function is 1, it follows that in this case

$$\mathfrak{I}(\mathbf{r}_1, \ldots, \mathbf{r}_{2m}) = \mathfrak{I}(\mathbf{r}_1, \ldots, \dot{\mathbf{r}}_{i_1}, \ldots, \dot{\mathbf{r}}_{j_1}, \ldots, \mathbf{r}_{2m}),$$

where the dots mean that $\mathbf{r}_{i_1}, \mathbf{r}_{j_1}$ have been omitted. The proof is now completed by induction.

4. Estimation of Moments

Lemma 4 *Suppose $k \geq 2$, $m \geq 1$ and $v \geq 0$. Suppose that for every $\mathbf{r}$ with $|\mathbf{r}| = v$ we are given an $\mathbf{r}$-function $f_{\mathbf{r}}$. Put*

$$F(\mathbf{x}) = \sum_{|\mathbf{r}|=v} f_{\mathbf{r}}(\mathbf{x}). \tag{4.1}$$

Then (2.5) holds.

Proof Let $M = M_{km}(v)$ be the maximum of $\int F^{2m}(\mathbf{x})\, d\mathbf{x}$, taken over all functions $F(\mathbf{x})$ of the type (4.1), where each $f_{\mathbf{r}}(\mathbf{x})$ is either an $\mathbf{r}$-function or is identically zero. We shall prove that

$$M_{km}(v) < (2m)^{m(2k-3)}(v+1)^{m(k-1)}. \tag{4.2}$$

Let the $f_{\mathbf{r}}$ be chosen such that M is attained for $F(\mathbf{x})$ given by (4.1). We then have

$$M = \int F(\mathbf{x})^{2m}\, d\mathbf{x} = \sum_{|\mathbf{r}_1|=v} \cdots \sum_{|\mathbf{r}_{2m}|=v} \mathfrak{I}(\mathbf{r}_1, \ldots, \mathbf{r}_{2m}), \tag{4.3}$$

with $\mathfrak{I}(\mathbf{r}_1, \ldots, \mathbf{r}_{2m})$ given by (3.2).

Suppose at first that $k = 2$. Then by Lemma 3 we may restrict ourselves to summands having $\mathbf{r}_{i_t} = \mathbf{r}_{j_t}$ $(t = 1, \ldots, m)$ for a certain division of $\{1, \ldots, 2m\}$ into pairs $(i_1, j_1), \ldots, (i_m, j_m)$. If this is the case, the integral $\mathfrak{I}(\mathbf{r}_1, \ldots, \mathbf{r}_{2m})$ is 0 if some of the functions $f_{\mathbf{r}_1}, \ldots, f_{\mathbf{r}_{2m}}$ are identically zero, and it is 1 otherwise. The number of divisions into pairs is $(2m-1)(2m-3)\cdots 3 \cdot 1 < (2m)^m$, and the number of possibilities for $\mathbf{r}_{i_1}, \ldots, \mathbf{r}_{i_m}$ is $(v+1)^m$. Thus for $k = 2$ we obtain the desired estimate

$$\int F(\mathbf{x})^{2m}\, d\mathbf{x} < (2m)^m (v+1)^m.$$

Now let $k > 2$. For each summand on the right-hand side of (4.3) put $r = \max(r_{1k}, \ldots, r_{2m,k})$, and write h for the number of components $r_{1k}, \ldots, r_{2m,k}$ which are equal to r. Then $\mathfrak{I}(\mathbf{r}_1, \ldots, \mathbf{r}_{2m}) = 0$ unless h is even, i.e., unless $h = 2u$ with $1 \leq u \leq m$. There are $\binom{2m}{2u}$ ways to pick $2u$ elements out of $\{1, \ldots, 2m\}$, and $\mathfrak{I}(\mathbf{r}_1, \ldots, \mathbf{r}_{2m})$ is invariant under permutations of $\mathbf{r}_1, \ldots, \mathbf{r}_{2m}$. Thus if the numbers u, v are always connected by $u + v = m$, then

$$M = \sum_{u=1}^{m} \binom{2m}{2u} \sum_{r=0}^{v} \sum\nolimits'_{2u} \sum\nolimits''_{2v} \mathfrak{I}(\mathbf{r}_1, \ldots, \mathbf{r}_{2u}, \mathbf{s}_1, \ldots, \mathbf{s}_{2v}),$$

where $\sum'_{2u}$ is the sum over $2u$-tuples $\mathbf{r}_1, \ldots, \mathbf{r}_{2u}$ with $|\mathbf{r}_1| = \cdots = |\mathbf{r}_{2u}| = v$ and $r_{1k} = \cdots = r_{2u,k} = r$, and $\sum''_{2v}$ is the sum over $2v$-tuples $\mathbf{s}_1, \ldots, \mathbf{s}_{2v}$ with $|\mathbf{s}_1| = \cdots = |\mathbf{s}_{2v}| = v$ and $s_{1k}, \ldots, s_{2v,k} < r$. Thus if

$$A_r(\mathbf{x}) = \sum\nolimits'^{r} f_{\mathbf{r}}(\mathbf{x}),$$

where the sum is over $\mathbf{r}$ with $|\mathbf{r}| = v$ and $r_k = r$, and if

$$B_r(\mathbf{x}) = \sum{}'' f_{\mathbf{r}}(\mathbf{x}),$$

where the sum is over $\mathbf{r}$ with $|\mathbf{r}| = v$ and $r_k < r$, then

$$M = \sum_{u=1}^{m} \binom{2m}{2u} \sum_{r=0}^{v} \int A_r^{2u}(\mathbf{x}) B_r^{2v}(\mathbf{x})\, d\mathbf{x}. \tag{4.4}$$

By Hölder's inequality,

$$\int A_r^{2u}(\mathbf{x}) B_r^{2v}(\mathbf{x})\, d\mathbf{x} \le \left(\int A_r^{2m}(\mathbf{x})\, d\mathbf{x}\right)^{u/m} \left(\int B_r^{2m}(\mathbf{x})\, d\mathbf{x}\right)^{v/m}. \tag{4.5}$$

The sum defining $A_r(\mathbf{x})$ is over $\mathbf{r} = (\bar{\mathbf{r}}, r)$ where $\bar{\mathbf{r}} = (r_1, \ldots, r_{k-1})$ runs through $(k-1)$-tuples with $|\bar{\mathbf{r}}| = v - r$. Hence for given x_k, the function $A_r(\mathbf{x})$ in $x_1, \ldots, x_{k-1}$ is of the type of $F(\mathbf{x})$, but with $k-1$ in place of k and $v - r$ in place of v. Thus if we proceed by induction on k, we may conclude that

$$\int A_r^{2m}(\mathbf{x})\, d\mathbf{x} < (2m)^{m(2k-5)}(v+1)^{m(k-2)}. \tag{4.6}$$

The function $B_r(\mathbf{x})$ is like $F(\mathbf{x})$, except that certain $f_{\mathbf{r}}$ in the sum (4.1) are replaced by 0. Thus by our definition of $M = M_{km}(v)$,

$$\int B_r^{2m}(\mathbf{x})\, d\mathbf{x} \le M. \tag{4.7}$$

Combining (4.4)–(4.7) we obtain

$$M < (v+1) \sum_{u=1}^{m} \binom{2m}{2u} ((2m)^{2k-5}(v+1)^{k-2})^u M^{v/m}. \tag{4.8}$$

Dividing by $M(v+1)$ and putting $M = L^m$ we get

$$(v+1)^{-1} < \sum_{u=1}^{m} \binom{2m}{2u} ((2m)^{2k-5}(v+1)^{k-2} L^{-1})^u.$$

So with $K = (2m)^{2k-5}(v+1)^{k-2}L^{-1}$ we have

$$(v+1)^{-1} < \sum_{u=1}^{m} \binom{2m}{2u} K^u < \sum_{u=1}^{m} \frac{1}{(2u)!} (4m^2K)^u.$$

Since

$$(v+1)^{-1} > \sum_{u=1}^{m} \frac{1}{(2u)!} (v+1)^{-u},$$

we obtain $4m^2K > (v+1)^{-1}$, or

$$L < (2m)^{2k-3}(v+1)^{k-1},$$

or (4.2).

5. Construction of an Auxiliary Function†

Lemma 5 *Suppose* $|\mathbf{r}| = v$ *with*

$$2^v \geq 2N. \tag{5.1}$$

Then there is an $\mathbf{r}$*-function* $f_{\mathbf{r}}$ *with*

$$\int f_{\mathbf{r}}(\mathbf{x})D(\mathbf{x})\,d\mathbf{x} \geq N \cdot 2^{-v-2k-1}. \tag{5.2}$$

Proof The integral in (5.2) may be decomposed into integrals over $\mathbf{r}$-boxes. We choose $f_{\mathbf{r}}(\mathbf{x})$ such that the integral over every $\mathbf{r}$-box is nonnegative.

If B is the $\mathbf{r}$-box given by $m_i 2^{-r_i} \leq x_i < (m_i+1)2^{-r_i}$ $(i = 1, \ldots, k)$, let B' be the smaller box $m_i 2^{-r_i} \leq x_i < (m_i + \frac{1}{2})2^{-r_i}$ $(i = 1, \ldots, k)$. Then

$$\int_B R_{\mathbf{r}}(\mathbf{x})D(\mathbf{x})\,d\mathbf{x} = \int_{B'} \sum_{\varepsilon_1=0}^{1} \cdots \sum_{\varepsilon_k=0}^{1} (-1)^{\varepsilon_1 + \cdots + \varepsilon_k} \times D(y_1 + \varepsilon_1 2^{-r_1-1}, \ldots, y_k + \varepsilon_k 2^{-r_k-1})\,d\mathbf{y}. \tag{5.3}$$

Now

$$\sum_{\varepsilon_1=0}^{1} \cdots \sum_{\varepsilon_k=0}^{1} (-1)^{\varepsilon_1 + \cdots + \varepsilon_k} Z(y_1 + \varepsilon_1 2^{-r_1-1}, \ldots, y_k + \varepsilon_k 2^{-r_k-1}) \tag{5.4}$$

is the number among the given N points that lie in the box $y_i \leq x_i < y_i + 2^{-r_i-1}$ $(i = 1, \ldots, k)$, which is contained in B. Thus this sum is 0 if B contains none of the given N points. On the other hand,

$$\sum_{\varepsilon_1=0}^{1} \cdots \sum_{\varepsilon_k=0}^{1} (-1)^{\varepsilon_1 + \cdots + \varepsilon_k} (y_1 + \varepsilon_1 2^{-r_1-1}) \cdots (y_k + \varepsilon_k 2^{-r_k-1}) = (-1)^k 2^{-|\mathbf{r}|-k} = (-1)^k 2^{-v-k}. \tag{5.5}$$

If B contains none of the given N points, then

$$\int_B R_{\mathbf{r}}(\mathbf{x})D(\mathbf{x})\,d\mathbf{x} = (-1)^{k+1} N 2^{-v-k} 2^{-v-k}$$

since B' has volume 2^{-v-k}. We observe that in view of (5.1), at least half of the 2^v $\mathbf{r}$-boxes B contain none of the given N points. Thus we obtain (5.2) for a suitably chosen $\mathbf{r}$-function $f_{\mathbf{r}}$.

Given v with (5.1), we construct an $\mathbf{r}$-function $f_{\mathbf{r}}$ according to Lemma 5 for every $\mathbf{r}$ with $|\mathbf{r}| = v$, and we define $F(\mathbf{x})$ by (4.1). Then since the number

† As noted in Section 2, our auxiliary function is almost the same as the one of Roth [4].

of k-tuples $\mathbf{r}$ with $|\mathbf{r}| = v$ is $> c_{12}(k)(v+1)^{k-1}$, we obtain

$$\int F(\mathbf{x})D(\mathbf{x})\,d\mathbf{x} > c_{13}(k)(v+1)^{k-1}2^{-v}N. \tag{5.6}$$

6. Proof of Theorem 1

Let v be the number with (2.6). Then (5.6) yields (2.1), and (2.5) is true by Lemma 4. Theorem 1 follows.

7. Proof of Theorem 2

Write $\exp x = e^x$ and

$$E_0(\mathbf{x}) = D(\mathbf{x})(v+1)^{-(k-1)/2}, \qquad G(\mathbf{x}) = F(\mathbf{x})(v+1)^{-(k-1)/2}, \tag{7.1}$$

where $F(\mathbf{x})$ is the auxiliary function constructed in Section 5.

Lemma 6 *For* $q > k - \frac{3}{2}$,

$$\int |G(\mathbf{x})| \exp(|G(\mathbf{x})|^{1/q})\,d\mathbf{x} < c_{14}(k, q).$$

Proof Since $\|G\|_\alpha$ is nondecreasing in α, we have $\|G\|_\alpha \le \|G\|_{2m}$ for $\alpha \le 2m$, whence by (2.5),

$$\int |G(\mathbf{x})|^\alpha\,d\mathbf{x} \le \left(\int G(\mathbf{x})^{2m}\,d\mathbf{x}\right)^{\alpha/2m} < (2m)^{\alpha(k-(3/2))}.$$

Therefore

$$\begin{aligned}\int |G(\mathbf{x})| \exp(|G(\mathbf{x})|^{1/q})\,d\mathbf{x} &= \sum_{h=0}^{\infty} \frac{1}{h!} \int |G(\mathbf{x})|^{1+(h/q)}\,d\mathbf{x} \\ &< \sum_{h=0}^{\infty} \frac{1}{h!} \langle 1 + (h/q)\rangle^{(1+(h/q))(k-(3/2))},\end{aligned} \tag{7.2}$$

where $\langle\beta\rangle$ denotes the next larger *even* integer to β. For large h, we have $\langle 1 + (h/q)\rangle < 2h$, and an exponent

$$(1 + (h/q))(k - \tfrac{3}{2}) < (1 - 2\delta)h$$

with $\delta = (1 - ((k - \frac{3}{2})/q)/4$. Since $h! > (2h)^{(1-\delta)h}$ for large h, a typical summand is $< (2h)^{-\delta h}$, so that the sum in (7.2) is convergent, say to $c_{14}(k, q)$.

With v determined by (2.6), we have

$$\int G(\mathbf{x})E_0(\mathbf{x})\,d\mathbf{x} > c_{15}(k) > 0 \tag{7.3}$$

by (5.6), (7.1). Pick $c_{16} = c_{16}(k, q)$ so large that $c_{14}e^{-c_{16}} < \frac{1}{2}c_{15}$. Let S be the set of $\mathbf{x}$ in U^k with

$$|E_0(\mathbf{x})| \le \exp(|G(\mathbf{x})|^{1/q} - c_{16}).$$

By Lemma 6 the integral of $G(\mathbf{x})E_0(\mathbf{x})$ over S is $< \frac{1}{2}c_{15}$. Hence the integral over the complement T of S is $> \frac{1}{2}c_{15}$, by (7.3). On T,

$$(\log |E_0(\mathbf{x})| + c_{16})^q > |G(\mathbf{x})|,$$

so that

$$\int |E_0(\mathbf{x})|\,|\log|E_0(\mathbf{x})| + c_{16}|^q\,d\mathbf{x} \ge \int_T |E_0(\mathbf{x})G(\mathbf{x})|\,d\mathbf{x} > \tfrac{1}{2}c_{15}.$$

Choose $c_{17} > 0$ so small that $z|\log z + c_{16}|^q < \frac{1}{4}c_{15}$ for $0 < z < c_{17}$. Then

$$\int_V |E_0(\mathbf{x})|\,|\log|E_0(\mathbf{x})| + c_{16}|^q\,d\mathbf{x} > \tfrac{1}{4}c_{15},$$

where V consists of $\mathbf{x} \in U^k$ with $|E_0(\mathbf{x})| \ge c_{17}$. We now choose $c_2 = c_2(k, q)$ so large that

$$c_2' = c_2((v+1)/\log N)^{(k-1)/2}$$

has

$$c_2' z|\log c_2' z|^q > 4c_{15}^{-1} z|\log z + c_{16}|^q$$

for $z \ge c_{17}$. With this value of c_2,

$$c_2 E(\mathbf{x}) = c_2 D(\mathbf{x})(\log N)^{-(k-1)/2} = c_2' E_0(\mathbf{x})$$

satisfies (1.3).

8. Estimation of Sums

We now turn to Theorem 3. For simplicity of notation, we shall assume that $k = 2$. The constants $\gamma_1, \gamma_2, \ldots$ will be positive and absolute.

Suppose we are given a discrete set of points in the quadrant $y_1 \ge 0$, $y_2 \ge 0$. For $\mathbf{x} = (x_1, x_2)$ in this quadrant, write $Z(\mathbf{x})$ for the number of points among the given discrete set that lie in the rectangle $0 \le y_1 < x_1$,

$0 \le y_2 < x_2$. Put $D(\mathbf{x}) = Z(\mathbf{x}) - Nx_1x_2$. Now if Q is a square

$$m_i \le x_i < m_i + 1 \qquad (i = 1, 2) \tag{8.1}$$

in our quadrant, the results proved above about U^2 remain true for Q. More precisely, if the number $N(Q)$ of points among the given discrete set in Q satisfies

$$2^v \ge 2N(Q), \tag{8.2}$$

then there is a function $F(\mathbf{x})$ defined on Q such that

$$\int_Q F(\mathbf{x})D(\mathbf{x})\,d\mathbf{x} > \gamma_1(v+1)2^{-v}N \tag{8.3}$$

(in analogy with (5.6)) and

$$\int_Q F^{2m}(\mathbf{x})\,d\mathbf{x} < (2m)^m(v+1)^m \qquad (m = 1, 2, \ldots) \tag{8.4}$$

(in analogy with (2.5)). For example, in order to derive (8.3), we note that the alternating sums (5.4) depend only on the points of the given discrete set that lie in Q.

Given a square Q determined by (8.1) and given a nonnegative integer μ, a *grid* $\Gamma(Q, \mu)$ will be a set of points $\mathbf{x} = (x_1, x_2)$ of the type

$$x_i = m_i + \xi_i + l_i 2^{-\mu} \qquad (i = 1, 2),$$

where ξ_1, ξ_2 are fixed with $0 \le \xi_1 < 2^{-\mu}$ $(i = 1, 2)$, and l_1, l_2 run independently through the integers $0, 1, \ldots, 2^\mu - 1$. The grid $\Gamma(Q, \mu)$ is contained in Q and the number of its points is

$$|\Gamma(Q, \mu)| = 4^\mu. \tag{8.5}$$

Because of the freedom in choosing ξ_1, ξ_2, there are infinitely many grids $\Gamma(Q, \mu)$ contained in Q.

Given integers $\mu > v \ge 0$, we may replace the integrals (8.3), (8.4) by sums over the points of a grid $\Gamma(Q, \mu)$. This is so because in the alternating sums (5.3)–(5.5) we never get outside the grid. We sum up our results in

Lemma 7 *Let Q be a square of the type* (8.1). *Let μ, v be integers with*

$$\mu > v \ge 0 \qquad \text{and} \qquad 2^v \ge 2N(Q). \tag{8.6}$$

Let a grid $\Gamma(Q, \mu)$ be given. Then there is a function $F(\mathbf{x})$ defined on $\Gamma(Q, \mu)$ with

$$|\Gamma(Q, \mu)|^{-1} \sum_{\mathbf{x} \in \Gamma(Q, \mu)} F(\mathbf{x})D(\mathbf{x}) > \gamma_1(v+1)2^{-v}N, \tag{8.7}$$

$$|\Gamma(Q, \mu)|^{-1} \sum_{\mathbf{x} \in \Gamma(Q, \mu)} F^{2m}(\mathbf{x}) < (2m)^m(v+1)^m \qquad (m = 1, 2, \ldots). \tag{8.8}$$

We note that $|F(\mathbf{x})| \leq v + 1$ since $F(\mathbf{x})$ was constructed as the sum of $v + 1$ r-functions.

More generally, we shall allow squares Q of the type

$$m_i 2^{-\lambda} \leq x_i < (m_i + 1)2^{-\lambda} \qquad (i = 1, 2), \tag{8.9}$$

where λ is a nonnegative integer. A grid $\Gamma(Q, \mu)$ will be a set of points $\mathbf{x} = (x_1, x_2)$ of the form

$$x_i = 2^{-\lambda}(m_i + \xi_i + l_i 2^{-\mu}) \qquad (i = 1, 2)$$

where ξ_1, ξ_2 are given with $0 \leq \xi_i < 2^{-\mu}$ and where l_1, l_2 run through 0, 1, ..., $2^{\mu} - 1$. Such a grid is contained in Q and its number of elements is given by (8.5).

Lemma 8 *Let Q be a square of the type* (8.9). *Let μ, v be integers satisfying* (8.6). *Let a grid $\Gamma(Q, \mu)$ be given. Then there is a function $F(\mathbf{x})$ defined on $\Gamma(Q, \mu)$ with* (8.8), *with*

$$|\Gamma(Q, \mu)|^{-1} \sum_{\mathbf{x} \in \Gamma(Q, \mu)} F(\mathbf{x})D(\mathbf{x}) > \gamma_1(v + 1)2^{-v-2\lambda}N, \tag{8.10}$$

and with

$$|F(\mathbf{x})| \leq v + 1. \tag{8.11}$$

Proof The dilation T with $T\mathbf{x} = 2^{\lambda}\mathbf{x}$ maps Q into a square Q' of side 1 and it maps $\Gamma(Q, \mu)$ into a grid $\Gamma(Q', \mu)$. If $\mathbf{P}$ is the given set of points, put $\mathbf{P}' = T(\mathbf{P})$ and define $Z'(\mathbf{x})$ with reference to $\mathbf{P}'$. Put $N' = 4^{-\lambda}N$ and $D'(\mathbf{x}) = Z'(\mathbf{x}) - N'x_1x_2$. Then

$$D'(T\mathbf{x}) = Z'(T\mathbf{x}) - N'4^{\lambda}x_1x_2 = Z(\mathbf{x}) - Nx_1x_2 = D(\mathbf{x}).$$

We apply Lemma 7 with $\Gamma(Q', \mu)$ in place of $\Gamma(Q, \mu)$, and with N', D' in place of N, D. We obtain a function $F'(\mathbf{x})$ defined on $\Gamma(Q', \mu)$. The function $F(\mathbf{x}) = F'(T\mathbf{x}) = F'(2^{\lambda}\mathbf{x})$ is defined on $\Gamma(Q, \mu)$ and has the desired properties.

Lemma 9 *Let $\lambda, u, v, Q, \Gamma(Q, \mu), F(\mathbf{x})$ be as in Lemma* 8. *Suppose $X > 4$. The number $\varphi(X)$ of points $\mathbf{x}$ of $\Gamma(Q, \mu)$ with*

$$|F(\mathbf{x})| > X(v + 1)^{1/2}$$

satisfies

$$\varphi(X) < |\Gamma(Q, \mu)| \exp(-2^{-4}X^2).$$

Proof We have

$$\varphi(X)|\Gamma(Q, \mu)|^{-1}X^{2m} < (2m)^m \qquad (m = 1, 2, \ldots)$$

by (8.8). Pick an integer m with

$$1 < (1/4e)X^2 < m \leq (1/2e)X^2.$$

Then

$$\varphi(X)|\Gamma(Q, \mu)|^{-1} < (2mX^{-2})^m \leq e^{-m} < \exp(-2^{-4}X^2).$$

9. Preparations for Theorem 3

The basic idea of the proof is as follows. For most squares Q of the type (8.9), $N(Q)$ should be not much larger than $N4^{-\lambda}$, where N is the number of our given points in U^2. For such a square Q, we may choose ν with $2^\nu \geq 2N(Q)$ such that 2^ν has the order of magnitude $N4^{-\lambda}$, and hence $2^{\nu+2\lambda}$ is about equal to N. Thus (8.10) becomes

$$|\Gamma(Q, \mu)|^{-1} \sum_{\mathbf{x} \in \Gamma(Q, \mu)} F(\mathbf{x})D(\mathbf{x}) > \gamma_2(\nu + 1), \tag{9.1}$$

for most squares Q. The auxiliary function $F(\mathbf{x})$ has $|F(\mathbf{x})| \leq \nu + 1$, but from Lemma 9 it is clear that it is usually not much larger than $(\nu + 1)^{1/2}$. If we knew that the summands in (9.1) where $|F(\mathbf{x})|$ is small compared to $\nu + 1$ give a large contribution, we could conclude that

$$|\Gamma(Q, \mu)|^{-1} \sum_{\mathbf{x} \in \Gamma(Q, \mu)} |D(\mathbf{x})|$$

is large. If we knew this to happen for many grids, we would ultimately be led to a good lower bound for $\| D \|_1$. It will therefore be necessary to pay attention to the case when the relatively few summands of (9.1) where $|F(\mathbf{x})|$ is almost as large as $\nu + 1$ give a large contribution. In this case there is a small subset Δ of $\Gamma(Q, \mu)$ such that

$$|\Gamma(Q, \mu)|^{-1} \sum_{\mathbf{x} \in \Delta} |D(\mathbf{x})| > \gamma_3 . \tag{9.2}$$

In order to go beyond such a constant to a function that tends to infinity with N, we shall have to apply Lemma 8 with different values of λ, μ, and ν.

We now proceed to carry out this program. Let ρ be the integer with

$$4N \leq 4^\rho < 16N. \tag{9.3}$$

Putting

$$\nu(u) = (12)^u(u!)^2 \qquad (u = 1, 2, \ldots), \tag{9.4}$$

we have

$$u4^{\nu(u-1)+1} \exp(-2^{-2}u^{-2}\nu(u)) < 4u \exp(2\nu(u-1) - 3\nu(u-1)) < 1 \tag{9.5}$$

for $u > 1$. Let t be an integer with

$$\nu(t) \leq 2\rho, \tag{9.6}$$

and write

$$\lambda(u) = \rho - \tfrac{1}{2}v(u), \qquad \mu(u) = v(u) + 1 \qquad (u = 1, \ldots, t). \tag{9.7}$$

Then $\lambda(u) + \mu(u) = \rho + \frac{1}{2}v(u) + 1$ is increasing in $1 \le u \le t$, and

$$2^{-v(u)-2\lambda(u)}N = 4^{-\rho}N > 2^{-4}. \tag{9.8}$$

A square Q will be written as Q^u if it is given by inequalities

$$m_i 2^{-\lambda(u)} \le x_i < (m_i + 1)2^{-\lambda(u)} \qquad (i = 1, 2)$$

with integers m_i in $0 \le m_i < 2^{\lambda(u)}$. For $1 \le v \le u \le t$, the number of squares Q^v contained in a given square Q^u is

$$A(v, u) = 4^{\lambda(v)-\lambda(u)}.$$

For $v \le u$ and a given square Q^u, write $A(v, Q^u)$ for the number of squares $Q^v \subseteq Q^u$ with

$$N(Q^v) \le 2N4^{-\lambda(v)}. \tag{9.9}$$

Clearly,

$$0 \le A(v, Q^u) \le A(v, u). \tag{9.10}$$

The right-hand side of (9.9) is $2N$ times the area of Q^v, while the average of $N(Q^v)$ over all squares Q^v is N times the area of Q^v. It follows that (9.9) must be true for at least half of the squares Q^v, i.e., for at least $\frac{1}{2}4^{\lambda(v)}$ squares Q^v. So for $v \le u$,

$$\sum_{Q^u} A(v, Q^u) \ge \tfrac{1}{2}4^{\lambda(v)}, \tag{9.11}$$

where the sum is over all squares Q^u.

For $1 \le u \le t$ and every square Q^u, put

$$h(Q^u) = \sum_{v=1}^{u} A(v, Q^u)/A(v, u), \tag{9.12}$$

so that by (9.10),

$$0 \le h(Q^u) \le u. \tag{9.13}$$

We shall write Γ^u for a grid $\Gamma(Q^u, \mu(u))$. The number of points of Γ^u is

$$B(u) = |\Gamma^u| = 4^{\mu(u)}. \tag{9.14}$$

Put

$$B(v, u) = B(u)B(v)^{-1} = 4^{\mu(u)-\mu(v)}.$$

For $1 \le v < u \le t$, the square Q^u is the disjoint union of $A(v, u)$ squares Q^v.

The grid $\Gamma^u = \Gamma(Q^u, \mu(u))$ has "mesh" $2^{-\lambda(u)-\mu(u)}$ (i.e., its points have horizontal and vertical distances of this size), and hence Γ^u is the union of $A(v, u)$ grids of the type $\Gamma(Q^v, \mu(u) + \lambda(u) - \lambda(v))$, which also have this mesh. In turn, since $\mu(u) + \lambda(u) - \lambda(v) > \mu(v)$, each grid $\Gamma(Q^v, \mu(u) + \lambda(u) - \lambda(v))$ is the disjoint union of $2^{\lambda(u)+\mu(u)-\lambda(v)-\mu(v)}$ grids $\Gamma(Q^v, \mu(v))$. We write all this up in

$$\Gamma^u = \bigcup_{Q^u \subset Q^v} \bigcup{}' \Gamma^v. \tag{9.15}$$

Here $\Gamma^u = \Gamma(Q^u, \mu(u))$, the outside union is over the $A(v, u)$ squares $Q^u \subset Q^v$, and the inside union $\bigcup'$ is over

$$2^{\lambda(u)+\mu(u)-\lambda(v)-\mu(v)} = B(v, u)A(v, u)^{-1}$$

grids $\Gamma^v = \Gamma(Q^v, \mu(v))$.

Given a grid Γ^u, write

$$g(\Gamma^u) = B(u)^{-1} \sum_{\mathbf{x} \in \Gamma^u} |D(\mathbf{x})|. \tag{9.16}$$

10. A Lemma

Lemma 10 *For $1 \le u \le t$ and a grid $\Gamma^u = \Gamma(Q^u, \mu(u))$,*

$$g(\Gamma^u) \ge \gamma_4 h(Q^u). \tag{10.1}$$

Proof We take

$$\gamma_4 = \gamma_1 2^{-6} \tag{10.2}$$

where γ_1 is the constant of Lemma 8.

We begin with $u = 1$, in which case

$$h(Q^1) = A(1, Q^1),$$

which is 0 or 1. The interesting case is when it is 1; then $N(Q^1) \le 2N4^{-\lambda(1)}$, or by (9.3), (9.7),

$$2N(Q^1) \le N4^{1-\lambda(1)} = N4^{1-\rho}2^{\nu(1)} \le 2^{\nu(1)}.$$

Thus (8.6) is true for $\mu = \mu(1)$, $\nu = \nu(1)$, $\Gamma(Q^1, \mu(1))$, and we may apply Lemma 8. Since $|F(\mathbf{x})| \le \nu + 1$, (8.10) yields

$$g(\Gamma^1) = |\Gamma^1|^{-1} \sum_{\mathbf{x} \in \Gamma^1} |D(\mathbf{x})| > \gamma_1 2^{-\nu(1)-2\lambda(1)} N > \gamma_1 2^{-4} > \gamma_4$$

by (9.8).

We now proceed to the induction from $u-1$ to u, where $2 \le u \le t$. By (9.15) with $v = u-1$,

$$g(\Gamma^u) = B(u-1, u)^{-1} \sum_{Q^{u-1} \subset Q^u} \sum_{\Gamma^{u-1}}{}' g(\Gamma^{u-1}), \tag{10.3}$$

where $\sum'$ is a sum over $B(u-1, u)A(u-1, u)^{-1}$ grids $\Gamma^{u-1} \subset Q^{u-1}$.

On the other hand, for $1 \le v \le u-1$, we have $A(v, u) = A(v, u-1)A(u-1, u)$ and

$$\begin{aligned} A(v, Q^u)/A(v, u) &= \sum_{Q^{u-1} \subset Q^u} A(v, Q^{u-1})/A(v, u) \\ &= A(u-1, u)^{-1} \sum_{Q^{u-1} \subset Q^u} A(v, Q^{u-1})/A(v, u-1). \end{aligned}$$

It follows that

$$h(Q^u) = A(u, Q^u) + A(u-1, u)^{-1} \sum_{Q^{u-1} \subset Q^u} h(Q^{u-1}). \tag{10.4}$$

It will be convenient to write this as

$$h(Q^u) = A(u, Q^u) + B(u-1, u)^{-1} \sum_{Q^{u-1} \subset Q^u} \sum_{\Gamma^{u-1}}{}' h(Q^{u-1}), \tag{10.5}$$

where the inner sum $\sum'$ is over $B(u-1, u)A(u-1, u)^{-1}$ grids $\Gamma^{u-1} \subset Q^{u-1}$, as in (10.3), and the summand $h(Q^{u-1})$ is independent of Γ^{u-1}.

Our inductive assumption yields $g(\Gamma^{u-1}) \ge \gamma_4 h(Q^{u-1})$. Comparing (10.3) and (10.5), we thus obtain the desired relation (10.1), *provided* $A(u, Q^u) = 0$. It remains to deal with the case when

$$A(u, Q^u) = 1. \tag{10.6}$$

Now the double sum in (10.3) and (10.5) is altogether over a set $\mathfrak{S}$ of $B(u-1, u)$ grids Γ^{u-1}. To deal with the case (10.6), it would suffice to construct a subset $\mathfrak{T}$ of $\mathfrak{S}$ such that (with the notation $h(\Gamma^{u-1}) = h(Q^{u-1})$ if $\Gamma^{u-1} = \Gamma(Q^{u-1}, \mu(u-1))$),

$$B(u-1, u)^{-1} \sum_{\Gamma^{u-1} \in \mathfrak{T}} (g(\Gamma^{u-1}) - \gamma_4 h(\Gamma^{u-1})) \ge \gamma_4 .$$

Since $h(Q^{u-1}) \le u-1$ by (9.13), it would suffice to have

$$B(u-1, u)^{-1} \sum_{\Gamma^{u-1} \in \mathfrak{T}} g(\Gamma^{u-1}) \ge \gamma_4 \, B(u-1, u)^{-1} u |\mathfrak{T}| + \gamma_4 ,$$

where $|\mathfrak{T}|$ is the number of elements of $\mathfrak{T}$; or

$$B(u)^{-1} \sum_{\Gamma^{u-1} \in \mathfrak{T}} \sum_{\mathbf{x} \in \Gamma^{u-1}} |D(\mathbf{x})| \ge \gamma_4 B(u-1, u)^{-1} u |\mathfrak{T}| + \gamma_4 .$$

Prime Ideal Decomposition in $F(\mu^{1/m})$, II†

WILLIAM YSLAS VÉLEZ

UNIVERSITY OF ARIZONA AND SANDIA LABORATORIES
TUCSON, ARIZONA ALBUQUERQUE, NEW MEXICO

1. Introduction

Let F be an algebraic number field, μ an integer in F, $x^m - \mu$ irreducible over F, and $\mathscr{P}$ a prime ideal in the ring of algebraic integers in F with $(m, \mathscr{P}) = 1$. We are interested in discovering how the ideal $\mathscr{P}$ decomposes when considered as an ideal in $F(\mu^{1/m})$. It was shown, in Mann and Vélez [2, p. 132], that we can reduce this problem to the situation where $(\mu, \mathscr{P}) = 1$. Under this assumption we have that $\mathscr{P}$ does not ramify in $F(\mu^{1/m})$. In Mann and Vélez [2] we also defined ${}_F\Psi_m(\mathscr{P})$, the counting function for the decomposition of $\mathscr{P}$ in $F(\mu^{1/m})$, where ${}_F\Psi_m(\mathscr{P})$ merely counts how many ideals there are of each degree in the decomposition of $\mathscr{P}$ in $F(\mu^{1/m})$. That is, if

$$ {}_F\Psi_m(\mathscr{P}) = \sum_{i=1}^{n} g_i[f_i], $$

then $\mathscr{P}$ factors in $F(\mu^{1/m})$ into g_i ideals of degree f_i, for $i = 1, \ldots, n$, and $m = \sum_{i=1}^{n} g_i f_i$.

† This work was supported in part by the U.S. Energy Research and Development Administration (ERDA), Contract No. AT(29-1)-789. The author is currently at Sandia Laboratories.

Let Q^* denote the nonzero rational numbers and Z the ring of integers and consider $Z(Q^*)$, the group ring of Q^* with coefficients in Z. Let us denote elements in $Z(Q^*)$ by $\sum_i n_i[r_i]$, where $n_i \in Z$, $r_i \in Q^*$. Then $Z(Z^*)$ is imbedded in a natural way in $Z(Q^*)$. Moreover, ${}_F\Psi_m(\mathscr{P}) = \sum g_i[f_i]$ can be considered as being an element in $Z(Z^*)$ since $g_i \in Z$ and $f_i \in Z^*$. Hence, we can define an addition and multiplication for counting functions by considering the counting functions as elements of $Z(Z^*)$.

In Mann and Vélez [2] we were able to explicitly compute ${}_F\Psi_{l^c}(\mathscr{P})$, where l is a prime, $(l\mu, \mathscr{P}) = 1$. Furthermore, we showed that if $m = \prod_{i=1}^{k} l_i^{c_i}$ and $l \mid N(\mathscr{P}) - 1$, where $N(\mathscr{P})$ denotes the norm of $\mathscr{P}$ over Q, then ${}_F\Psi_m(\mathscr{P}) = \prod_{i=1}^{k} {}_F\Psi_{l_i^{c_i}}(\mathscr{P})$.

In this paper we shall give a recursive procedure for computing ${}_F\Psi_m(\mathscr{P})$ in terms of the counting functions ${}_F\Psi_{l^c}(\mathscr{P})$, where l is a prime. Furthermore, we shall investigate the phenomenon where

$$ {}_F\Psi_m(\mathscr{P}) = \prod_{i=1}^{s} {}_F\Psi_{l_i^{c_i}}(\mathscr{P}), \qquad m = \prod_{i=1}^{s} l_i^{c_i}. $$

2. Theorems and Proofs

By $o(\mu)$ modulo $\mathscr{P}$ we shall mean the multiplicative order of μ in the group of units modulo $\mathscr{P}$.

Lemma 1 *Let $x^m - \mu$ be irreducible over F, l a prime, $(l, m) = 1$. If $l^n \parallel o(\mu)$ modulo $\mathscr{P}$ (where $l^n \parallel b$ means $l^n \mid b$, $l^{n+1} \nmid b$), then $l^n \parallel o(\mu^{1/m})$ modulo $\mathscr{P}_i$, where $\mathscr{P}_i$ is any prime divisor of $\mathscr{P}$ in $F(\mu^{1/m})$.*

Proof The proof follows by applying Theorem 2 in Mann and Vélez [2] and induction. ∎

Let $l \mid N(\mathscr{P}) - 1$. Then from Rules 1–4 in Mann and Vélez [2], we see that ${}_F\Psi_{l^c}(\mathscr{P})$ depends only on three parameters, namely, l^c, l^k, where $l^k \parallel N(\mathscr{P}) - 1$, and $l^n = (o(\mu), l^k)$. Set $N(\mathscr{P}) = p^f$.

If $l \nmid N(\mathscr{P}) - 1$, then ${}_F\Psi_{l^c}(\mathscr{P})$ depends only on three parameters, namely, r, l^c and l^w, where $l^w \parallel p^{fr} - 1$ and r is the order of p^f modulo l. To emphasize this, we set ${}_F\Psi_{l^c}(\mathscr{P}) = C(l^c, o(\mu), p^f)$, where C is computed according to Rules 1–5 in Mann and Vélez [2].

From the above comments we have the following: If $(q, l) = 1$, then

$$ C(l^c, q \cdot o(\mu), p^f) = C(l^c, o(\mu), p^f). \tag{1} $$

If $(q, l) = 1$ and $l \mid p^f - 1$, then

$$ C(l^c, o(\mu), p^{fq}) = C(l^c, o(\mu), p^f) \tag{2} $$

since if $l^k \parallel p^f - 1$, $k > 0$, then $l^k \parallel p^{fq} - 1$.

If $l \nmid (p^f - 1)$, r is the order of p^f modulo l and $(q, lr) = 1$, then

$$C(l^c, o(\mu), p^{fq}) = C(l^c, o(\mu), p^f). \tag{3}$$

On using Theorem 4 from Mann and Vélez [2], we can also show, by induction, that ${}_F\Psi_m(\mathscr{P})$ depends only on m, $N(\mathscr{P}) = p^f$, and the order of μ modulo $\mathscr{P}$. Hence, we set ${}_F\Psi_m(\mathscr{P}) = C(m, o(\mu), p^f)$.

If $(q, m) = 1$, then we have

$$C(m, q \cdot o(\mu), p^f) = C(m, o(\mu), p^f). \tag{4}$$

Let $m = q_1^{e_1} \cdots q_s^{e_s} l_1^{c_1} \cdots l_n^{c_n}$, where the q_i, l_j are distinct primes, $q_i \mid p^f - 1$, $l_i \nmid p^f - 1$ and r_i is the order of p^f modulo l_i. If $(q, q_i) = (q, r_j l_j) = 1$, for all i, j, then

$$C(m, o(\mu), p^f) = C(m, o(\mu), p^{fq}). \tag{5}$$

Given $x^m - \mu$ and $N(\mathscr{P}) = p^f$, write $m = q_1^{e_1} \cdots q_s^{e_s} l_1^{c_1} \cdots l_n^{c_n}$, where q_i, l_j are distinct primes, $q_i \mid p^f - 1$, $l_j \nmid p^f - 1$, r_j is the order of p^f modulo l_j, and $q_i^{k_i} \parallel p^f - 1$. (6)

Lemma 2 *Let $x^m - \mu$ be irreducible over F, $(m\mu, \mathscr{P}) = 1$, and ${}_F\Psi_m(\mathscr{P}) = \sum_i g_i[f_i]$, then $f_i \mid mR_n$, where $R_n = \prod_{j=1}^n r_j$, for each i.*

Proof We shall prove this by induction on n. Assume that $n = 0$ in (6) above. Then by Theorem 5 in Mann and Vélez [2], we have that ${}_F\Psi_m(\mathscr{P}) = \prod_{i=1}^s {}_F\Psi_{q_i^{e_i}}(\mathscr{P})$. But, from Rules 1–5 in Mann and Vélez [2], the theorem holds for each ${}_F\Psi_{q_i^{e_i}}(\mathscr{P})$, hence it holds for m.

Assume that the assertion is true for $n = k$ and $m = q_1^{e_1} \cdots q_s^{e_s} l_1^{c_1} \cdots l_{k+1}^{c_{k+1}} = m_1 l_{k+1}^{c_{k+1}}$. Let ${}_F\Psi_{m_1}(\mathscr{P}) = \sum g_i[f_i]$, then by induction, $f_i \mid (m_1 \cdot R_k)$, for each f_i that appears in the sum ${}_F\Psi_{m_1}(\mathscr{P})$.

Let $\mathscr{P}_i$ be an ideal factor of $\mathscr{P}$ in $F_1 = F(\mu^{1/m_1})$ of relative degree f_i, for each i. Then by Theorem 4 in [2], we have that

$${}_F\Psi_m(\mathscr{P}) = (\sum g_i[f_i])_{F_1}\Psi_{l_{k+1}^{c_{k+1}}} \qquad (\mathscr{P}_i).$$

But if ${}_{F_1}\Psi_{l_{k+1}^{c_{k+1}}}(\mathscr{P}_i) = \sum_j g_{ij}[f_{ij}]$, then $f_{ij}] l_{k+1}^{c_{k+1}} \cdot r_{k+1}$ by Rules 1–5 in Mann and Vélez [2], for each j. Hence $f_t f_{ij} \mid m_1 R_k l_{k+1}^{c_{k+1}} r_{k+1}$. So $f_t f_{ij} \mid mR_{k+1}$. However, $f_t f_{ij}$ is an arbitrary term in ${}_F\Psi_m(\mathscr{P})$, so the induction is complete. ∎

Lemma 3 *Let $x^m - \mu$ be irreducible over F, $(m\mu, \mathscr{P}) = 1$, $m = m_1 l^c$, $(m_1, l) = 1$, l a prime, and ${}_F\Psi_{m_1}(\mathscr{P}) = \sum g_i[f_i]$. If $l \mid p^f - 1$ and $(l, f_i) = 1$, for all i, then ${}_F\Psi_m(\mathscr{P}) = {}_F\Psi_{m_1}(\mathscr{P}) \cdot {}_F\Psi_{l^c}(\mathscr{P})$. If $l \nmid p^f - 1$ and $(rl, f_i) = 1$, for all i, then ${}_F\Psi_m(\mathscr{P}) = {}_F\Psi_{m_1}(\mathscr{P}) \cdot {}_F\Psi_{l^c}(\mathscr{P})$.*

Proof Let $F_1 = F(\mu^{1/m_1})$ and $\mathscr{P}_i$ a prime factor of $\mathscr{P}$ in F_1 of relative

degree f_i, for each i. Then by Theorem 4 in Mann and Vélez [2], we have that ${}_F\Psi_m(\mathscr{P}) = \sum g_i[f_i] \cdot {}_{F_1}\Psi_{l^c}(\mathscr{P}_i)$. But, ${}_{F_1}\Psi_{l^c}(\mathscr{P}_i) = C(l^c, o(\mu^{1/m_1}), p^{ff_i})$. By Lemma 1, if $l^n \| o(\mu)$, then $l^n \| o(\mu^{1/m_1})$ since $(m_1, l) = 1$. Hence $C(l^c, o(\mu^{1/m_1}), p^{ff_i}) = C(l^c, o(\mu), p^{ff_i})$.

If $l \mid p^f - 1$ and $l^w \| p^f - 1$, then $l^w \| p^{ff_i} - 1$, since $(f_i, l) = 1$.

If $l \nmid p^f - 1$ and $l^w \| p^{fr} - 1$, then r is the order of p^{ff_i} and $l^w \| p^{ff_i r} - 1$, since $(f_i, rl) = 1$.

Hence $C(l^c, o(\mu), p^{ff_i}) = C(l^c, o(\mu), p^f) = {}_F\Psi_{l_c}(\mathscr{P})$. So we have that for each i, ${}_{F_1}\Psi_{l^c}(\mathscr{P}_i) = {}_F\Psi_{l^c}(\mathscr{P})$. Hence ${}_F\Psi_m(\mathscr{P}) = {}_F\Psi_{m_1}(\mathscr{P}) \cdot {}_F\Psi_{l^c}(\mathscr{P})$. ∎

Theorem 1 *Let $x^m - \mu$ be irreducible over F, $m = m_1 l^c$, l a prime, $(m\mu, \mathscr{P}) = (m_1, l) = 1$, and l is the largest divisor of m such that $l \nmid p^f - 1$, then*

$$ {}_F\Psi_m(\mathscr{P}) = {}_F\Psi_{m_1}(\mathscr{P}) + C(m_1, o(\mu), p^{fr})({}_F\Psi_{l^c}(\mathscr{P}) - 1[1]). $$

Proof Let $m = q_1^{e_1} \cdots q_s^{e_s} l_1^{c_1} \cdots l_n^{c_n} = m_1 l^c$, where $l^c = l_n^{c_n}$. Since $r_i \mid l_i - 1$, we have that $r_i < l_i < l$, $i < n$, hence $(l, R_{n-1}) = 1$. Hence $(l, m_1 R_{n-1}) = 1$, where $R_{n-1} = \prod_{i=1}^{n-1} r_i$.

Let $F_1 = F(\mu^{1/l})$, then ${}_F\Psi_l(\mathscr{P}) = 1[1] + (l-1)/r[r]$. If $c = 1$, then

$$ \begin{aligned} {}_F\Psi_m(\mathscr{P}) &= {}_F\Psi_{m_1}(\mathscr{P}) + (l-1)/r[r] \cdot C(m_1, o(\mu), p^{fr}) \\ &= {}_F\Psi_{m_1}(\mathscr{P}) + C(m_1, o(\mu), p^{fr})({}_F\Psi_l(\mathscr{P}) - 1[1]). \end{aligned} $$

Hence, the theorem is true for $c = 1$. Assume it is true for $c = k$ and let $m = m_1 l^{k+1}$. Then

$$ {}_F\Psi_m(\mathscr{P}) = {}_F\Psi_{m_1 l^k}(\mathscr{P}) + (l-1)/r[r] \cdot C(m_1 l^k, l \cdot o(\mu), p^{fr}). $$

By Lemma 2, if $C(m_1, l \cdot o(\mu), p^{fr}) = \sum g_i[f_i]$, then $f_i \mid m_1 R_{n-1}$. Hence $(f_i, l) = 1$, so by Lemma 3 we have that

$$ C(m_1 l^k, l \cdot o(\mu), p^{fr}) = C(m_1, o(\mu), p^{fr}) C(l^k, l \cdot o(\mu), p^{fr}). $$

Hence

$$ \begin{aligned} {}_F\Psi_m(\mathscr{P}) &= {}_F\Psi_{m_1}(\mathscr{P}) + C(m_1, o(\mu), p^{fr})({}_F\Psi_{l^k}(\mathscr{P}) - 1[1]) \\ &\quad + (l-1)/r[r] C(m_1, o(\mu), p^{fr}) C(l^k, l \cdot o(\mu), p^{fr}) \\ &= {}_F\Psi_{m_1}(\mathscr{P}) + C(m_1, o(\mu), p^{fr}) \\ &\quad \cdot ({}_F\Psi_{l^k}(\mathscr{P}) + (l-1)/r[r] C(l^k, l \cdot o(\mu), p^{fr}) - 1[1]) \\ &= {}_F\Psi_{m_1}(\mathscr{P}) + C(m_1, o(\mu), p^{fr})({}_F\Psi_{l^{k+1}}(\mathscr{P}) - 1[1]), \end{aligned} $$

by Lemma 3 of [2]. So the induction is complete. ∎

Theorem 1 gives a recursive procedure for writing ${}_F\Psi_m(\mathscr{P})$ in terms of the counting functions of the divisors of m. That is, if $m = q_1^{e_1} \cdots q_s^{e_s} l_1^{c_1} \cdots$

$l_n^{c_n} = m_1 l_n^{c_n}$, as in (6), where $l_1 < l_2 < \cdots < l_n$, then by Theorem 1

$$ {}_F\Psi_m(\mathscr{P}) = {}_F\Psi_{m_1}(\mathscr{P}) + C(m_1, o(\mu), p^{fr_n})({}_F\Psi_{l_n^{cn}}(\mathscr{P}) - 1[1]). $$

Note, however, that ${}_F\Psi_{m_1}(\mathscr{P})$ has exactly $n-1$ primes dividing m and not dividing $p^f - 1$, $C(m_1, o(\mu), p^{fr_n})$ has no more than $n-1$ primes dividing m and not dividing $p^{fr_n} - 1$, while ${}_F\Psi_m(\mathscr{P})$ has exactly n primes dividing m and not dividing $p^f - 1$. Hence, this procedure can now be applied to ${}_F\Psi_{m_1}(\mathscr{P})$ and $C(m_1, o(\mu), p^{fr_n})$.

Example 1 If $n = 1$, then

$$ {}_F\Psi_m(\mathscr{P}) = {}_F\Psi_{m_1}(\mathscr{P}) + C(m_1, o(\mu), p^{fr_1})({}_F\Psi_{l_1^{c_1}}(\mathscr{P}) - 1[1]). $$

However, by Theorem 5 in Mann and Vélez [2], we have that

$$ {}_F\Psi_m(\mathscr{P}) = \prod_{i=1}^{s} {}_F\Psi_{q_i^{e_i}}(\mathscr{P}) + \left(\prod_{i=1}^{s} C(q_i^{e_i}, o(\mu), p^{fr_1})\right)({}_F\Psi_{l_1^{c_1}}(\mathscr{P}) - 1[1]). $$

So, ${}_F\Psi_m(\mathscr{P})$ is expressed in terms of the known counting functions of its prime divisors.

Example 2 $m = q_1^{e_1} \cdots q_s^{e_s} l_1^{c_1} l_2^{c_2} = m_1 l_1^{c_1} l_2^{c_2}$, $l_1 < l_2$, then

$$ \begin{aligned} {}_F\Psi_m(\mathscr{P}) &= {}_F\Psi_{m_1 l_1^c}(\mathscr{P}) + C(m_1 l_1^{c_1}, o(\mu), p^{fr_2})({}_F\Psi_{l_2^{c_2}}(\mathscr{P}) - 1[1]) \\ &= {}_F\Psi_{m_1}(\mathscr{P}) + C(m_1, o(\mu), p^{fr_1})({}_F\Psi_{l_1^{c_1}}(\mathscr{P}) - 1[1]) \\ &\quad + C(m_1 l_1^{c_1}, o(\mu), p^{fr_2})({}_F\Psi_{l_2^{c_2}}(\mathscr{P}) - 1[1]). \end{aligned} $$

Now, the first two terms can be factored as in Example 1. We consider two cases: (1) $l_1 \mid p^{fr_2} - 1$, (2) $l_1 \nmid p^{fr_2} - 1$ and the order of p^{fr_2} modulo l_1 is r_1', then in case 1,

$$ C(m_1 l_1^{c_1}, o(\mu), p^{fr_2}) = \prod_{i=1}^{s} C(q_1^{e_1}, o(\mu), p^{fr_2}) \cdot C(l_1^{c_1}, o(\mu), p^{fr_2}), $$

by Theorem 5 in Mann and Vélez [2].

In case 2, we must apply Theorem 1 and we have

$$ \begin{aligned} C(m_1 l_1^{c_1}, o(\mu), p^{fr_2}) &= C(m_1, o(\mu), p^{fr_2}) \\ &\quad + C(m_1, o(\mu), p^{fr_2 r_1'})(C(l_1^{c_1}, o(\mu), p^{fr_2}) - 1[1]). \quad \blacksquare \end{aligned} $$

Lemma 4 *Let $x^{l^c} - \mu$ be irreducible over F, $(l\mu, \mathscr{P}) = 1$, $l^k \parallel p^f - 1$, $k \geq 1$, and $l^n = (o(\mu), l^k)$, then ${}_F\Psi_{l^c}(\mathscr{P}) = l^c[1]$ iff $c \leq k - n$.*

Proof The lemma is proved by referring to Rules 1–4 in Mann and Vélez [2]. If Rule 1 applies, then

$$ {}_F\Psi_{l^c}(\mathscr{P}) = l^{\min\{c,\, k-n\}}[l^{\max\{0,\, c-k+n\}}] = l^c[1] \qquad \text{iff} \quad c \leq k - n. $$

Rule 2 cannot apply here since $k = 1 = n$. If Rules 3 or 4 apply, then $n = 0$ and the assertion is obvious. $\blacksquare$

Lemma 5 *If λ is an integer in F, $(\lambda, \mathscr{P}) = 1$, then for each m there is an irreducible polynomial $x^m - \mu$ such that $\mu \equiv \lambda \pmod{\mathscr{P}}$.*

Proof Let $\mathscr{P}'$ be a prime ideal in F such that $(\mathscr{P}', \mathscr{P}) = 1$. Then, we can find an ideal $\mathscr{A}$ such that $(\mathscr{A}, \mathscr{P}\mathscr{P}') = 1$ and $\mathscr{P}'\mathscr{A} = (\pi)$ (see Mann [1, p. 50]). Hence $\mathscr{P}' \| \pi$. Since $(\mathscr{P}', \mathscr{P}) = 1$, we can solve the system of congruences $x \equiv \lambda/\pi \pmod{\mathscr{P}}$, $x \equiv 1 \pmod{\mathscr{P}'}$. Let β be such a solution and set $\mu = \beta\pi$. Then $\mu \equiv \lambda \pmod{\mathscr{P}}$. Furthermore, since $\mathscr{P}' \| \mu$, we have that $x^m - \mu$ is an Eisenstein polynomial, and hence, $x^m - \mu$ is irreducible for all m. ∎

In Lemma 3 we had the situation where ${}_F\Psi_{m_1 l^c}(\mathscr{P}) = {}_F\Psi_{m_1}(\mathscr{P}) \cdot {}_F\Psi_{l^c}(\mathscr{P})$. The next theorem, in fact, characterizes this phenomenon.

Theorem 2 *Let $m = m_1 l^c$, $(m_1, l) = 1$, $x^m - \mu$ irreducible over F, then ${}_F\Psi_m(\mathscr{P}) = {}_F\Psi_{m_1}(\mathscr{P}) \cdot {}_F\Psi_{l^c}(\mathscr{P})$, for all such m_1 iff $l \mid p^f - 1$ and $c \leq k - n$, where k and n are as in Lemma 4.*

Proof Assume first that $l \mid p^f - 1$ and $c \leq k - n$. Let $F_1 = F(\mu^{1/l^c})$, then by Lemma 4, we have that ${}_F\Psi_{l^c}(\mathscr{P}) = l^c[1]$. Hence, if $\mathscr{P}_1$ is any factor of $\mathscr{P}$ in F_1, then

$$ {}_F\Psi_m(\mathscr{P}) = l^c_{F_1}\Psi_{m_1}(\mathscr{P}_1) = l^c C(m_1, o(\mu^{1/l^c}), p^f) = l^c C(m_1, o(\mu), p^f), $$

since $(l, m_1) = 1$. Hence ${}_F\Psi_m(\mathscr{P}) = l^c_F\Psi_{m_1}(\mathscr{P}) = {}_F\Psi_{l^c}(\mathscr{P})_F\Psi_{m_1}(\mathscr{P})$.

Next, assume that ${}_F\Psi_m(\mathscr{P}) = {}_F\Psi_{m_1}(\mathscr{P}) \cdot {}_F\Psi_{l^c}(\mathscr{P})$, for all m_1, $(m_1, l) = 1$. Assume first that $l \nmid p^f - 1$ and let r be the order of p^f modulo l. Let l_1 be a prime such that $l_1 \nmid p^f - 1$ and $(r_1, r) \neq 1$, where r_1 is the order of p^f modulo l_1. By assumption,

$$ {}_F\Psi_{ll_1}(\mathscr{P}) = {}_F\Psi_l(\mathscr{P}) \cdot {}_F\Psi_{l_1}(\mathscr{P}) = {}_F\Psi_l(\mathscr{P})(1[1] + (l_1 - 1)/r_1[r_1]). $$

Now, let $F_1 = F(\mu^{1/l_1})$ and $\mathscr{P}_0$ a prime factor of $\mathscr{P}$ in F_1 of degree 1, $\mathscr{P}_1$ a prime factor of $\mathscr{P}$ in F_1 of degree r_1, then

$$ \begin{aligned} {}_F\Psi_{ll_1}(\mathscr{P}) &= {}_{F_1}\Psi_l(\mathscr{P}_0) + (l_1 - 1)/r_1[r_1] \cdot C(l, o(\mu), p^{fr_1}) \\ &= {}_F\Psi_l(\mathscr{P}) + (l_1 - 1)/r_1[r_1]C(l, o(\mu), p^{fr_1}) \\ &= {}_F\Psi_l(\mathscr{P}) \cdot {}_F\Psi_{l_1}(\mathscr{P}) = {}_F\Psi_l(\mathscr{P}) + (l_1 - 1)/r_1[r_1] \cdot {}_F\Psi_l(\mathscr{P}). \end{aligned} $$

Hence, ${}_F\Psi_l(\mathscr{P}) = C(l, o(\mu), p^{fr_1})$, but this is impossible since $(r, r_1) \neq 1$. So, if ${}_F\Psi_m(\mathscr{P}) = {}_F\Psi_{m_1}(\mathscr{P}) \cdot {}_F\Psi_{l^c}(\mathscr{P})$, for all m_1 prime to l, then $l \mid p^f - 1$. Since $l \mid p^f - 1$, let $l^k \| p^f - 1$ and choose k_1 so that $k_1 \geq k$ and $c \leq k_1 - n$. Set $K = k_1 - k$. Let l_1 be a prime so that $(l_1, p^f - 1) = 1$ and $l^K \mid r_1$, where r_1 is the order of p^f modulo l_1. By Lemma 5, we know that there exists an irreducible polynomial $x^{l^c l_1} - \lambda$, where $\lambda \equiv \mu \pmod{\mathscr{P}}$. So $o(\lambda) = o(\mu)$.

Hence

$$_F\Psi_{l^c l_1}(\mathscr{P}) = {}_F\Psi_{l^c}(\mathscr{P}) + (l_1 - 1)/r_1[r_1]C(l^c, o(\mu), p^{fr_1}).$$

Since $l^K \mid r_1$ and $l^k \parallel p^{fr} - 1$, we have that $l^{k_1} \mid p^{fr_1} - 1$. But $c \leq k_1 - n$, hence by Lemma 4, we have that $C(l^c, o(\mu), p^{fr_1}) = l^c[1]$. Hence

$$\begin{aligned} {}_F\Psi_{l^c l_1}(\mathscr{P}) &= {}_F\Psi_{l^c}(\mathscr{P}) + (l_1 - 1)/r_1[r] \cdot l^c[1] \\ &= {}_F\Psi_{l^c}(\mathscr{P})_F\Psi_{l_1}(\mathscr{P}) = {}_F\Psi_{l^c}(\mathscr{P}) + (l_1 - 1)/r_1[r_1]_F\Psi_{l^c}(\mathscr{P}), \end{aligned}$$

so ${}_F\Psi_{l^c}(\mathscr{P}) = l^c[1]$, hence $c \leq k - n$, by Lemma 4, and the theorem is proven. ∎

Theorem 3 *Let $x^m - \mu$ be irreducible over F and m is written as in* (6), *then*

$$_F\Psi_m(\mathscr{P}) = \prod_{i=1}^{s} {}_F\Psi_{q_i^{e_i}}(\mathscr{P}) \cdot \prod_{j=1}^{n} {}_F\Psi_{l_j^{c_j}}(\mathscr{P})$$

if (a) $(r_i, r_j) = (r_i, l_j) = 1$, *and* (b) *for each i, either $(q_j, r_i) = 1$ or $e_j \leq k_j - n_j$, for each j, where $q_j^{n_j} \parallel o(\mu)$ modulo $\mathscr{P}$.*

Proof Assume that $(r_i, r_j) = (r_i, l_j) = 1$ and $(q_j, r_i) = 1$ or $e_j \leq k_j - n_j$. We shall induct on the number of prime factors of m. If m is a power of a prime, then we are done. Hence assume that m has $k + 1$ distinct prime factors and the theorem is true for k prime factors. If $e_j \leq k_j - n_j$, then by Lemma 4 we have that ${}_F\Psi_m(\mathscr{P}) = {}_F\Psi_{m_1}(\mathscr{P}) \cdot {}_F\Psi_{q_j^{e_j}}(\mathscr{P})$, where $m_1 = m/q_j^{e_j}$. Then induction applies to ${}_F\Psi_{m_1}(\mathscr{P})$ and the theorem is proven. Hence, we may assume that $e_j > k_j - n_j$, for all j. Then we must have that for each i and j, $(r_i, q_j) = 1$. If $n = 0$, then we are done by Theorem 5 in Mann and Vélez [2]. Hence, assume that $n \neq 0$. Without loss of generality, we may assume that $l_n > l_i$, $i < n$. Then, by Theorem 1, we have that

$$_F\Psi_m(\mathscr{P}) = {}_F\Psi_{m_1}(\mathscr{P}) + C(m_1, o(\mu), p^{fr_n})({}_F\Psi_{l_n^{c_n}}(\mathscr{P}) - 1[1]).$$

where $m_1 = m/l_n^{c_n}$. But $(r_n, r_i l_i) = 1 = (r_n, q_j)$, for all j, $i < n$. Hence, by (5), we have that

$$C(m_1, o(\mu), p^{fr_n}) = C(m_1, o(\mu), p^f) = {}_F\Psi_{m_1}(\mathscr{P}),$$

so ${}_F\Psi_m(\mathscr{P}) = {}_F\Psi_{m_1}(\mathscr{P}) \cdot {}_F\Psi_{l_n^{c_n}}(\mathscr{P})$, so, we can apply the induction hypothesis to ${}_F\Psi_{m_1}(\mathscr{P})$, and the induction is complete. ∎

Conjecture We conjecture that if

$$_F\Psi_m(\mathscr{P}) = \prod_{i=1}^{s} {}_F\Psi_{q_i^{e_i}}(\mathscr{P}) \cdot \prod_{j=1}^{n} {}_F\Psi_{l_j^{c_j}}(\mathscr{P}),$$

the numerical conditions, (a) and (b), in Theorem 3 hold, that is, that Theorem 3 is actually a characterization of this phenomena.

REFERENCES

[1] Henry B. Mann, "Introduction to Algebraic Number Theory." The Ohio State Univ. Press, Columbus, Ohio, 1955.
[2] Henry B. Mann and William Yslas Vélez, Prime ideal decomposition in $F(\mu^{1/m})$, *Monatsh. Math.* **81** (1976), 131–139.

AMS (MOS) 1970 subject classifications: 12A45, 12B10.

Rational Quadratic Forms and Orthogonal Designs

WARREN WOLFE†

QUEEN'S UNIVERSITY
KINGSTON, ONTARIO, CANADA‡

Orthogonal designs were introduced as a generalization of Hadamard arrays and their existence has been studied by several authors. This work has led to some intricate and elaborate methods and results, but, to date, no general method has been developed. In this paper we claim to isolate the algebraic properties of orthogonal designs and show that the existence of these designs is dependent upon the equivalence of quadratic forms. We give strong necessary conditions for the existence of orthogonal designs in orders $2^r \cdot n_0$, n_0 *odd,* $r = 0, 1, 2,$ *or* 3.

Definition An *orthogonal design in order n and of type* $(u_1, \ldots, u_s)$ *on the commuting variables* $x_1, \ldots, x_s$ is an $n \times n$ matrix X with entries from $\{0, \pm x_1, \ldots, \pm x_s\}$ such that $XX^t = (\sum_1^s u_i x_i^2) I_n$.

Alternatively, each row of X contains u_i entries of the type $\pm x_i$ and the rows are formally orthogonal. Such matrices were first described in Geramita *et al.* [2] and have been very useful for determining the existence of

† This paper is based on the author's doctoral dissertation written at Queen's University, Kingston, Ontario, Canada, under the supervision of Dr. A. V. Geramita.

‡ Present address: Department of Mathematics, Royal Roads Military College, Victoria, British Columbia, Canada.

weighing matrices and, in particular, Hadamard matrices. (See Geramita *et al.* [2], Geramita and Wallis [3] or Germaita and Wallis [3a].)

If X is as above, we may write $X = \sum_1^s A_i x_i$ where the A_i are the coefficient matrices. Then the A_i are 0, ± 1 matrices of order n such that:

(i) the A_i are disjoint, i.e., if $A_i = (a_{kl})$, $A_j = (b_{pq})$ $(i \neq j)$, then $a_{kl} b_{kl} = 0$ for every k, l;
(ii) $A_i A_i^t = u_i I_n$, $1 \leq i \leq s$;
(iii) $A_i A_j^t + A_j A_i^t = 0$, $i \neq j$.

It has been demonstrated that each of the above properties sets a strong criteria for the existence of an orthogonal design. In this paper, however, we shall examine only the algebraic properties, namely (ii) and (iii). For this purpose we make the following definition:

Definition A *rational family in order n and of type* $[u_1, \ldots, u_s]$ is a family of $n \times n$ rational matrices $\{A_1, \ldots, A_s\}$ such that (ii) and (iii) above are satisfied.

Surely a rational family reflects the algebraic properties of an orthogonal design, and the existence of an orthogonal design will imply the existence of a rational family in the same order and of the same type.

If $\{A_1, \ldots, A_s\}$ is a rational family as above, then:

(i) $\{a_i A_i, 1 \leq i \leq s\}$, where $a_i \in Q$ is a rational family in order n and of type $[a_1^2 u_1, \ldots, a_s^2 u_s]$;
(ii) $\{A_1 + A_2, A_3, \ldots, A_s\}$ is a rational family in order n and of type $[u_1 + u_2, u_3, \ldots, u_s]$;
(iii) if P and Q are $n \times n$ rational matrices such that $PP^t = pI_n$ and $QQ^t = qI_n$, then $\{PA_iQ, 1 \leq i \leq s\}$ is a rational family in order n and of type $[pu_1 q, \ldots, pu_s q]$.

Thus, one may "translate" a rational family in the same order and so change the type numbers to a certain extent.

The first theorem for rational families limits the number of matrices in such a family and was first noted in Geramita and Pullman [1] and later described in terms of orthogonal designs.

Theorem 1 (Radon–Geramita–Pullman) *There exists a rational family in order n with s members if and only if* $s \leq \rho(n)$ *(the Radon function), where, if* $n = 2^{4a+b} \cdot n_0$, n_0 *odd,* $0 \leq b < 4$, *then* $\rho(n) = 8a + 2^b$.

Necessity in the above theorem is proved using Radon's result on the maximal number of anticommuting, skew-symmetric, orthogonal real matrices in order n (see Radon [6]). Sufficiency is given by Geramita and Pullman [1], who have shown that, for a given n, there exists a rational

family in order n with $\rho(n)$ members and of type $[1, 1, \ldots, 1]$. In fact, the matrices in their rational families are disjoint $0, \pm 1$ matrices.

The Radon function is easily computable; for example, $\rho(2n_0) = 2$, $\rho(4n_0) = 4$, $\rho(8n_0) = 8$, $\rho(16n_0) = 9, \ldots$, where n_0 is odd.

Further existence theorems for orthogonal designs have been found involving type numbers. In certain orders, Geramita and Wallis have shown that these type numbers were closely related to sums of squares (see Geramita *et al.* [2] and Geramita and Wallis [3].) We shall show that, more precisely, rational families (and hence orthogonal designs) rely on the equivalence of rational quadratic forms. We refer the reader to Serre [7] for particulars and shall establish notation and definitions.

Let f be an n-dimensional quadratic form over Q, and let M_f be the uniquely determined symmetric $n \times n$ rational matrix such that $f(X) = X^t M_f X$.

Two quadratic forms f and g are said to be *equivalent* if there exists an invertible matrix P such that $M_g = PM_f P^t$. We write $f \simeq g$ to denote this equivalence. Every quadratic form f is equivalent to a diagonal form, i.e., there exists an invertible matrix P such that $PM_f P^t$ is the diagonal matrix $\mathrm{dg}(a_1, \ldots, a_n)$ for some $a_i \in Q$. We denote this diagonal form as $\langle a_1, \ldots, a_n \rangle$. Let $n \cdot \langle 1 \rangle$ denote the form given by the identity matrix I_n.

If $f = \langle a_1, \ldots, a_n \rangle$, we let $\delta(f)$ be the *discriminant* of f, i.e., the image of $\prod_1^n a_i$ in the group Q^*/Q^{*2}.

Let p be a prime and let Q_p denote the field of p-adic numbers. If a, b are in Q_p, the *p-adic Hilbert symbol* of a and b is (note a, b nonzero)

$$(a, b)_p = \begin{cases} 1 & \text{if } \exists x, y, z \text{ in } Q_p \text{ (not all zero) such that } ax^2 + by^2 - z^2 = 0 \\ -1 & \text{otherwise.} \end{cases}$$

If $f = \langle a_1, \ldots, a_n \rangle$ is a rational quadratic form, then the *p-adic Hasse invariant* of f is $s_p(f) = \prod_{i<j} (a_i, a_j)_p$.

We can now state the main theorem on the classification of rational quadratic forms.

Theorem 2 (weak Hasse–Minkowski) *f and g are equivalent rational quadratic forms if and only if they have the same dimension, the same discriminant, the same Hasse invariant at each prime, and the same number of positive terms in equivalent diagonal forms.*

Theorem 3 *If $n = 1, 2, 4,$ or 8, then there exists a rational family in order n and of type $[u_1, \ldots, u_n]$ if and only if $n \cdot \langle 1 \rangle \simeq \langle u_1, \ldots, u_n \rangle$.*

Proof If $\{A_i, 1 \le i \le n\}$ is a rational family in order n and of type $[u_1, \ldots, u_n]$, let v_i be the vector in Q^n that corresponds to the first row of A_i. Then, by the properties of a rational family, the v_i form an orthogonal basis for Q^n

where the norm of v_i (in the usual Euclidean sense) is u_i. Let P be the $n \times n$ matrix whose ith row is v_i. Then $PP^t = \mathrm{dg}(u_1, \ldots, u_n)$ and, consequently, $n \cdot \langle 1 \rangle \simeq \langle u_1, \ldots, u_n \rangle$.

Conversely, if $n \cdot \langle 1 \rangle \simeq \langle u_1, \ldots, u_n \rangle$, then there exists an invertible $n \times n$ matrix $P = (p_{ij})$ such that $PI_nP^t = \mathrm{dg}(u_1, \ldots, u_n)$. Let $\{B_i,\ 1 \leq i \leq n\}$ be the Geramita–Pullman rational family in order n and of type $[1, \ldots, 1]$. (Note that in Theorem 1, $\rho(n) = n$ if and only if $n = 1, 2, 4$, or 8.) (See Taussky [9] for a discussion of the 1, 2, 4, or 8 problem.)

Let $A_i = \sum_{j=1}^{n} p_{ij}B_j$. Then it is a straightforward verification to show that $\{A_i,\ 1 \leq i \leq n\}$ is a rational family in order n and of type $[u_1, \ldots, u_n]$.

The force of the above theorem is realized when one uses the following reduction theorem proved by Shapiro using his classification of similarities of quadratic forms.

Theorem 4 (Shapiro, [8]) *If $n = 2^m \cdot n_0$, n_0 odd, then there exists a rational family in order n if and only if there exists a rational family in order 2^m of the same type.*

In [8], Shapiro proves the above theorem for $m = 1, 2$, or 3. In a recent private communication, he has proved the general result.

We may now apply the above theorems to some particular cases of rational families.

Theorem 5 (i) *If n is odd, then there exists a rational family in order n and of types $[a]$ if and only if a is a square.*

(ii) *If $n \equiv 2 \pmod 4$, then there exists a rational family in order n and of type $[a, b]$ if and only if ab is a square and a and b are both sums of two rational squares.*

We note that the above results were already known in the context of weighing matrices and orthogonal designs (see Geramita *et al.* [2]).

Proof (i) follows directly by applying Theorems 3 and 4 and equating the discriminants of the forms $\langle a \rangle$ and $\langle 1 \rangle$.

(ii) Again by Theorems 3 and 4, we need only establish when $\langle a, b \rangle \simeq \langle 1, 1 \rangle$. Using Hasse–Minkowski and some standard Hilbert symbol arguments, one can show that this equivalence exists if and only if the stated conditions on a and b hold.

Theorem 6 *If $n \equiv 4 \pmod 8$, then there exists a rational family in order n and of type:*

(i) $[a, b, c, d]$ *if and only if $abcd$ is a square and, at every prime p, $s_p(\langle a, b, c, d \rangle) = 1$;*

(ii) $[a, b, c]$ *if and only if, at every prime p, $s_p(\langle a, b, c \rangle)(-1, abc)_p = 1$;*

(iii) $[a, b]$ *if and only if* ab *is a sum of three squares.*

(iv) $[a]$ *always.*

Proof (i) follows directly from Theorems 2–4.

(ii) By Theorem 4, we may reduce to order 4. We have seen that the existence of the rational family is equivalent to the existence of a 4×4 matrix P such that $PP^t = \mathrm{dg}(a, b, c, x)$ for some $x \in Q$. In terms of quadratic forms, $4\langle 1\rangle \simeq \langle a, b, c, x\rangle$. By equating discriminants, one sees that x must be abc, and the condition of (ii) will follow by equating the Hasse invariants.

(iii) was originally shown by Geramita and Wallis using a Pfaffian argument [3]. However, as in (ii), one may see that the existence of the rational family is equivalent to the existence of a rational number x such that $4 \cdot \langle 1\rangle \simeq \langle a, b, x, abx\rangle$. Using standard arguments, one can show that such an x exists if and only if ab is a sum of three squares.

(iv) follows since, for any positive a, $4 \cdot \langle 1\rangle \simeq \langle a, a, a, a\rangle$.

Theorem 7 *If* $n \equiv 8 \pmod{16}$, *then there exists a rational family in order* n *and:*

(i) *with five or fewer members always;*

(ii) *of type* $[a_1, \ldots, a_8]$ *if and only if* $\prod_1^8 a_i$ *is a square and, at every prime* p, $s_p(\langle a_1, \ldots, a_8\rangle) = 1$;

(iii) *of type* $[a_1, \ldots, a_7]$ *if and only if, at every prime* p,

$$s_p(\langle a_1, \ldots, a_7\rangle)(-1, \textstyle\prod_1^7 a_i)_p = 1;$$

(iv) *of type* $[a_1, \ldots, a_6]$ *where* $a_1 a_2 a_3 a_4$ *is a square and* $s_p(\langle a_1, \ldots, a_4\rangle) = 1$ *if and only if* $a_5 a_6$ *is a sum of three squares.*

Proof Clearly (ii) and (iii) are the analogous of (i) and (ii) in Theorem 6 and are proven similarly.

In (iv), the additional hypothesis on $a_1, \ldots, a_4$ merely states that a rational family of type $[a_1, \ldots, a_4]$ exists in order 4. If $a_5 a_6$ is a sum of three squares, then a rational family of type $[a_5, a_6]$ exists in order 4. By tensoring the members of one family with I_2 and of the other with $\left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$, one then constructs the required rational family in order 8. The converse argument is similar to that used for (iii) in Theorem 6.

(i) requires a slightly different technique and we thank Shapiro for sharing a critical observation. If a, b, c, d, and e are any positive rational numbers, then let $\delta = \mathrm{discriminant}\langle a, b, c, d, e\rangle$. Since every positive rational number is represented by $f = \langle a, b, c, d, e\rangle$ [7, p. 37], δ is represented by f and, hence $f \simeq \langle \delta, x, y, z, xyz\rangle$ for some x, y, z in Q [7, p. 33]. A routine check will show that $8 \cdot \langle 1\rangle \simeq \langle \delta, x, y, z, xyz, \delta xy, \delta xz, \delta yz\rangle$ and, hence, for some quadratic form g, $8 \cdot \langle 1\rangle \simeq f \perp g$. The conclusion of (i) now follows.

The only question left unanswered in orders $8 \cdot n_0$, where n_0 is odd, is

what happens in (iv) of Theorem 8 if one removes the additional hypothesis. That is, if $a_1, \ldots, a_6$ are positive rational numbers of which no four satisfy completely the added hypothesis, does there exist a rational family in order 8 and of type $[a_1, \ldots, a_6]$?

Also of interest are the orders divisible by 2^r, where $r > 3$. In personal communication, Shapiro indicates that he has proved the following result:

Theorem 8 (Shapiro) *If* $n \equiv 16 \pmod{32}$, *then there exists a rational family in order n and of type* $(a_1, \ldots, a_9)$ *if and only if at every prime p,* $s_p(a_1, \ldots, a_9) = 1$.

This result is the first of its kind in orders $16 \cdot n_0$, if n_0 is odd, and will eliminate many 9-tuples as possible types of rational families in these orders. Shapiro has shown that a relationship between rational families and quadratic forms does indeed exist in every order. His result now gives a complete solution of the problem of existence of rational families in every order. (We indicate, in an appendix, the orthogonal designs in order 16 on nine variables whose existence is still in doubt.)

We have noted that an orthogonal design gives rise to a rational family in the same order and of the same type. Hence all necessary conditions for the existence of rational families are necessary conditions for the existence of orthogonal designs. In the appendices to this paper we give some indication of how these results help determine the existence of orthogonal designs in some particular orders.

The sufficiency of the conditions above for rational families would indicate that our approach has exhausted the algebraic properties of orthogonal designs. However, there are also combinatorial results that prohibit the existence of orthogonal designs of certain types and orders, and we refer the reader to a sequence of papers which have recently appeared by Geramita, Wallis, *et al.* For the purpose of this paper, we shall note one such result and show how it may be blended with the above theorems to achieve a more complete picture.

Theorem 9 (Geramita–Verner; see [4]) *If* $n \equiv 0 \pmod{4}$, *then there exists an orthogonal design in order n and of type* $(u_1, \ldots, u_s)$ *where* $\sum_1^s u_i = n - 1$ *if and only if there exists an orthogonal design in order n and of type* $(1, u_1, \ldots, u_s)$.

We couple this theorem with Theorem 6 and obtain the following result:

Theorem 10 *If* $n \equiv 4 \pmod{8}$ *and if there exists an orthogonal design in order n and of type:*

(i) (a, b, c) *where* $a + b + c = n - 1$, *then abc is a square and, at every prime p,* $s_p(\langle a, b, c\rangle) = 1$;

(ii) (a, b) *where* $a + b = n - 1$, *then at every prime p,* $(a, b)_p = 1$.

Similarly, combining Theorems 7 and 9, we get

Theorem 11 *If* $n \equiv 8 \pmod{16}$ *and if there exists an orthogonal design in order* n *and of type:*

(i) $(a_1, \ldots, a_7)$ *where* $\sum_1^7 a_i = n - 1$, *then* $\prod_1^7 a_i$ *is a square and, at every prime* p, $s_p(\langle a_1, \ldots, a_7\rangle) = 1$;

(ii) $(a_1, \ldots, a_6)$ *where* $\sum_1^6 a_i = n - 1$, *then, at every prime* p,

$$\left(-1, \prod_1^6 a_i\right)_p s_p(\langle a_1, \ldots, a_6\rangle) = 1;$$

(iii) $(a_1, \ldots, a_5)$ *where* $\prod_1^4 a_i$ *is a square,* $\sum_1^5 a_i = n - 1$, *and, at every prime* p, $s_p(\langle a_1, \ldots, a_4\rangle) = 1$, *then* a_5 *is a sum of three squares;*

(iv) $(a_1, \ldots, a_5)$ *where* $\prod_1^3 a_i$ *is a square,* $\sum_1^5 a_i = n - 1$, *and, at every prime* p, $s_p(\langle a_1, a_2, a_3\rangle) = 1$, *then* $a_4 a_5$ *is a sum of three squares.*

Examples of tuples which are eliminated by Theorems 10 and 11 as types of orthogonal designs are easy to find. For example, in order 20, the tuple (1, 2, 16) certainly satisfies condition (ii) in Theorem 6, but does not meet the condition (i) of Theorem 10. Similarly, the tuple (1, 1, 1, 1, 1, 1, 17) is not the type of an orthogonal design in order 24 since it fails to satisfy condition (i) of Theorem 11.

Appendix I

In this appendix we wish to update the status of known orthogonal designs in order 20. We use as a base the list given by Geramita and Verner [4].

The following 4-tuples are easily eliminated using Theorem 6 (i): (1, 1, 2, 16), (1, 1, 5, 8), (1, 1, 5, 13), (1, 1, 8, 10), (1, 2, 6, 11), (1, 2, 2, 8), and (2, 3, 7, 8).

We apply (ii) of the same theorem to the 3-tuples in doubt and find that the following tuples fail at the indicated prime:

(1, 3, 9), (1, 3, 10), (1, 3, 16), (1, 4, 6), (1, 6, 13), (2, 5, 6), (2, 6, 11), (3, 4, 10), (3, 7, 10)	at $p = 3$	(1, 2, 10), (1, 5, 13), (1, 8, 10), (5, 6, 7)	at $p = 5$
		(1, 5, 8), (2, 3, 8), (2, 7, 8)	at $p = 2$
(1, 3, 11), (3, 4, 11)	at $p = 11$	(2, 3, 13)	at $p = 13$

Similarly, the tuples (1, 2, 16), (3, 16), and (6, 13) are eliminated by Theorem 10.

J. Wallis reports in private communication that designs of type (3, 3, 6, 6), (1, 3, 14), (3, 6, 8), (2, 5, 7), and (7, 10) have been found in order 20. Using Theorem 13 of Geramita *et al.* [2], we have found designs of the following types where we indicate the first rows of the circulant matrices used:

type (1, 4, 5, 5):

$a\ d\ 0\ 0\ -d \qquad -d\ c\ 0\ 0\ c \qquad c\ d\ b\ -b\ d \qquad 0\ c\ b\ b\ -c$

type (1, 2, 2, 9):

$a\ b\ 0\ 0\ -b \qquad b\ b\ b\ 0\ 0 \qquad c\ d\ b\ -b\ 0 \qquad d\ -c\ 0\ b\ -b$

type (1, 2, 8, 9):

$a\ b\ c\ -c\ -b \qquad b\ b\ b\ c\ -c \qquad c\ d\ b\ -b\ c \qquad d\ -c\ -c\ b\ -b$

type (1, 4, 13):

$a\ c\ -c\ c\ -c \qquad 0\ c\ -c\ -c\ -c \qquad 0\ c\ b\ b\ -c \qquad b\ c\ c\ c\ -b$

At present, it is still unknown whether the following tuples are types of designs in order 20:

(1, 3, 6, 8) (5, 5, 9)
(1, 4, 4, 9) (3, 7, 8)
(1, 5, 5, 9)
(2, 2, 5, 5)

Appendix II

We should like to disclose the early status of orthogonal designs on four variables in order 28. Using Theorems 6 and 9 we can eliminate all 4-tuples except the 73 listed below (this list has been verified by an APL search on a Burroughs 6700 computer as programmed by J. Verner):

(1, 1, 1, 1)✓	(1, 3, 6, 18)	(2, 4, 8, 9)
(1, 1, 1, 4)✓	(1, 4, 4, 4)✓	(2, 5, 5, 8)✓
(1, 1, 1, 9)✓	(1, 4, 4, 9)✓	(2, 8, 8, 8)
(1, 1, 1, 16)✓	(1, 4, 4, 16)	(2, 8, 9, 9)
(1, 1, 1, 25)✓	(1, 4, 5, 5)✓	(3, 3, 3, 3)✓
(1, 1, 2, 2)✓	(1, 4, 8, 8)	(3, 3, 3, 12)
(1, 1, 2, 8)✓	(1, 4, 9, 9)	(3, 3, 6, 6)
(1, 1, 2, 18)	(1, 4, 10, 10)	(3, 4, 6, 8)
(1, 1, 4, 4)✓	(1, 5, 5, 9)✓	(3, 6, 8, 9)
(1, 1, 4, 9)✓	(1, 8, 8, 9)	(4, 4, 4, 4)✓

(1, 1, 4, 16)	(2, 2, 2, 2)✓	(4, 4, 4, 9)
(1, 1, 5, 5)✓	(2, 2, 2, 8)✓	(4, 4, 4, 16)
(1, 1, 8, 8)	(2, 2, 2, 18)	(4, 4, 5, 5)✓
(1, 1, 9, 9)✓	(2, 2, 4, 4)✓	(4, 4, 8, 8)
(1, 1, 10, 10)	(2, 2, 4, 9)	(4, 4, 9, 9)✓
(1, 1, 13, 13)	(2, 2, 4, 16)	(4, 4, 10, 10)
(1, 2, 2, 4)✓	(2, 2, 5, 5)✓	(4, 5, 5, 9)
(1, 2, 2, 9)✓	(2, 2, 8, 8)✓	(5, 5, 5, 5)✓
(1, 2, 2, 16)	(2, 2, 9, 9)	(5, 5, 8, 8)
(1, 2, 3, 6)✓	(2, 2, 10, 10)	(5, 5, 9, 9)
(1, 2, 4, 8)✓	(2, 3, 4, 6)	(6, 6, 6, 6)
(1, 2, 4, 18)	(2, 3, 6, 9)	(7, 7, 7, 7)✓
(1, 2, 6, 12)	(2, 4, 4, 8)✓	
(1, 2, 8, 9)✓	(2, 4, 4, 18)	
(1, 3, 6, 8)	(2, 4, 6, 12)	

The ✓ indicates those tuples that are the types of orthogonal designs constructed by:

(i) direct sum of designs in orders 16 and 12;
(ii) designs in order 14 and the amicable pair of types (1, 1); (1, 1) in order 2; see construction 22 of [2];
(iii) Baumert–Hall array of type (7, 7, 7, 7); see Wallis *et al.* [10, p. 261];
(iv) construction 16 of [2];
(v) Golay sequences; see [3a].

Appendix III

Shapiro's result in Theorem 8 is the first algebraic restriction on the type numbers of orthogonal designs in order 16. Below we list all 25 possible types of designs on 9 variables in order 16 not eliminated by Theorems 8 and 9.

(1, 1, 1, 1, 1, 1, 1, 1, 1)✓	(1, 1, 1, 1, 1, 1, 1, 4, 5)
(1, 1, 1, 1, 1, 1, 1, 1, 2)	(1, 1, 1, 1, 1, 1, 2, 2, 2)
(1, 1, 1, 1, 1, 1, 1, 1, 3)	(1, 1, 1, 1, 1, 1, 2, 2, 3)
(1, 1, 1, 1, 1, 1, 1, 1, 4)	(1, 1, 1, 1, 1, 1, 2, 2, 4)
(1, 1, 1, 1, 1, 1, 1, 1, 5)	(1, 1, 1, 1, 1, 1, 2, 2, 6)
(1, 1, 1, 1, 1, 1, 1, 1, 6)	(1, 1, 1, 1, 1, 1, 2, 3, 5)
(1, 1, 1, 1, 1, 1, 1, 1, 8)	(1, 1, 1, 1, 1, 1, 2, 4, 4)
(1, 1, 1, 1, 1, 1, 1, 2, 2)	(1, 1, 1, 1, 1, 2, 2, 2, 2)
(1, 1, 1, 1, 1, 1, 1, 2, 4)	(1, 1, 1, 1, 1, 2, 2, 3, 4)

(1, 1, 1, 1, 1, 1, 1, 2, 7)	(1, 1, 1, 1, 1, 2, 3, 3, 3)
(1, 1, 1, 1, 1, 1, 1, 3, 4)	(1, 1, 1, 1, 2, 2, 2, 2, 2)
(1, 1, 1, 1, 1, 1, 1, 3, 6)	(1, 1, 1, 1, 2, 2, 2, 2, 4)
	(1, 1, 2, 2, 2, 2, 2, 2, 2)✓

✓ indicates that a design of that type exists in order 16 (see [2]).

Combining Theorems 8 and 9, one may also eliminate the following 8-tuples as types of orthogonal designs in order 16.

(1, 1, 1, 1, 1, 3, 3, 4)	(1, 1, 1, 2, 2, 2, 3, 3)
(1, 1, 1, 1, 2, 2, 2, 5)	(1, 1, 2, 2, 2, 2, 2, 3)

REFERENCES

[1] A. V. Geramita and N. J. Pullman, A theorem of Hurwitz and Radon and orthogonal projective modules, *Proc. Amer. Math. Soc.* **42** (1974), 51–56.

[2] A. V. Geramita, J. M. Geramita, and J. S. Wallis, Orthogonal designs, to appear, *J. Linear and Multilinear Alg.*

[3] A. V. Geramita and J. S. Wallis, Orthogonal designs IV. Existence questions, *J. Combinatorial Theory Ser. A* **19** (1975), 66–83.

[3a] A. V. Geramita and J. S. Wallis, Orthogonal designs II, to appear, *Aequationes Math.*

[4] A. V. Geramita and J. H. Verner, Orthogonal designs with zero diagonal, to appear, *Canad. J. Math.* **28** (1976), 215–224.

[5] M. Plotkin, Decomposition of Hadamard matrices, *J. Combinatorial Theory Ser. A* **12** (1972), 127–130.

[6] J. Radon, Linear Scharen Orthogonaler Matrizen, *Abh. Math. Sem. Univ. Hamburg.* **1** (1922), 1–14.

[7] J. P. Serre, "A Course in Arithmetic," Springer-Verlag, New York, 1973.

[8] D. B. Shapiro, Similarities, quadratic forms, and Clifford algebras, Ph.D. Thesis, Univ. California, Berkeley, 1974.

[9] O. Taussky, (1, 2, 4, 8)-sums of squares and Hadamard matrices, "Combinatorics," Proc. Symp. in Pure Math., Amer. Math. Society, Providence, Rhode Island, 1971, pp. 229–233.

[10] W. D. Wallis, A. P. Street, and J. S. Wallis, "Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices," Lecture Notes, Vol. 292, Springer-Verlag, Berlin–Heidelberg–New York, 1972.

AMS (MOS) 1970 subject classifications: 05B30, 15A66.

On Finite Projective Planes of Lenz–Barlotti Class I3

JILL C. D. S. YAQUB

THE OHIO STATE UNIVERSITY
COLUMBUS, OHIO

We study the existence of finite planes of Lenz–Barlotti class I3, *in particular for orders* $n \leqslant 250$. *By extending a result of W. M. Kantor, we are able to exclude certain values of n that were not hitherto rejected. We show that* $n \neq 9$ *by direct calculation, and list all* $n \leq 250$ *for which the existence question is undecided. We also consider finite planes of class* I3 *whose additive loop has both inverse properties; in this case further orders can be excluded, in particular* $n = 25$ *and those n with* $n - 1 = 3^r$, $2(3^r)$, $3p$ *or* $6p$, *where p is a prime* > 3.

While finite planes of Lenz–Barlotti class I4 have been studied extensively, not much is known about finite planes of the related class I3, even for small values of the order. (Planes of both types have recently been surveyed by Kantor [6, 7]. There is no known finite example of either class.) The purpose of the present paper is to give a slight extension of a theorem of Kantor [6, Theorem 6.3], and to investigate the existence of planes of class I3 for specific values of the order n, where $n \leqslant 250$. Basic information concerning projective planes can be found in Dembowski [2], and Pickert [9]; we use the coordinate system of [9]. The principal results on finite planes of class I3 are summarized in Theorems A and B.

Theorem A *Let* π *be a plane of class* I3 *with finite order n. Let the*

coordinate quadrangle VUOE be chosen so that π *is* (V, OU) *and* (U, OV) *transitive, and let R be the corresponding ternary ring. Then:*

(i) *R is linear, multiplication is associative, and R satisfies the distributive law* $a(b + c) = ab + ac$. *The multiplicative group* R^* *is not commutative, the additive loop* $(R, +)$ *is not associative, and R does not satisfy the distributive law* $(b + c)a = ba + ca$.

(ii) R^* *contains at most one involution.*

(iii) *The Sylow 2-groups of* R^* *are cyclic or generalized quaternion.*

(iv) *If n is even and if p is a prime that divides* $n - 1$, *then there exist integers x, y, z, not all zero, such that* $nx^2 + (-1)^{(p-1)/2}py^2 = z^2$.

(v) *Let* $G = R^* \times R^*$, *let* $D = \{(a, b) \in G \mid b = a + 1\}$, $G_1 = \{1\} \times R^*$, $G_2 = R^* \times \{1\}$, *and* $G_3 = \{(r, r) \mid r \in R^*\}$. *Then* $|D| = n - 2$ *and*

$$\left(\sum_{d \in D} d\right)\left(\sum_{d \in D} d^{-1}\right) = n + \sum_{g \in G} g - \sum_{g \in G_1} g - \sum_{g \in G_2} g - \sum_{g \in G_3} g,$$

where the sums are taken in the rational group algebra QG of G.

(vi) *If* R^* *admits a noncyclic abelian 2-group as a homomorphic image, then n is a square.*

(vii) $n - 1$ *is not a power of* 2 *if* $n \neq 9$.

Proofs of the statements in (i) can be found in [9, §3.5]. Statement (ii) follows from the Ostrom–Lüneburg theorem [2, p. 120], and (iii) follows from (ii) (Burnside [1, p. 132]). Statements (iv) and (v) are proved by Hughes ([5, Theorem 3.2]; [4, §III. 1] respectively), and (vi), (vii) by Kantor [6, Theorem 6.3 and Corollary 6.4]. Note that only one distributive law is necessary for the proof of (v).

If $a \in (R, +)$, let $a + (-a) = 0$. Then $(R, +)$ is said to have the *right*, (*left*), *inverse property* if and only if, for all $a, b \in (R, +)$, $(b + a) + (-a) = b$ $(a + (-a + b) = b$, respectively).

Theorem B *Let* π *be a plane of class* I3 *with finite order n, coordinatized as in Theorem A. Suppose that* $(R, +)$ *has both inverse properties. Then:*

(i) $(-1) + 1 = 0, (-1)^2 = 1$, *and* $a(-1) = (-1)a = -a$ *for all* $a \in R$.

(ii) $(R, +)$ *is commutative.*

(iii) *If* $a^2 = 1$, *then* $a = 1$ *or* -1.

(iv) *Let* $a \neq 1$. *Then* $a + 1 = (-1)a^2 \Leftrightarrow a^3 = 1$.

(v) *If* $a^3 = b^3 = 1$, *if* $a, b \neq 1$, *and if* $ab = ba$, *then* $b = a$ *or* a^{-1}.

(vi) *The Sylow 3-groups of* R^* *are cyclic.*

(vii) $n - 1 \neq 3^r$ *or* $2(3^r)$.

(viii) *n is even* $\Leftrightarrow 1 + 1 = 0$.

(ix) *If* 3 *divides* n, *then* $1 + 1 = -1$; *if* $1 + 1 = -1$, *then* $n \equiv 1$ *or* 3 (mod 6).

(x) $n \not\equiv 0 \pmod 6$.

(xi) $n \not\equiv 2 \pmod 4$.

(xii) $n \not\equiv 15$ *or* $21 \pmod{24}$.

To prove (i), observe that $1 = 1 + (-1 + 1)$ by the left inverse property, whence $-1 + 1 = 0$. Then $(-1)^2 + (-1) = 0$, by the distributive law, so that $(-1)^2 = 1$. Thus, by Theorem A(ii), $a(-1) = (-1)a$ for all $a \in R$, and $a(-1) = -a$ by the distributive law. (This slight change in the proof of [6, Theorem 2.7(i)] is required because R now has only one distributive law.) Statements (ii)–(v) are proved in Kantor [6, Theorem 2.7, (ii)–(v)]. Note that the proof of Theorem 2.7(v) uses commutativity only in the subgroup $\langle a, b\rangle$, and hence proves the present statement (v). (The statement of Theorem 2.7(v), omitted in Kantor [6], can be found in Kantor [7].) Now (vi) follows from (v) (Burnside [1, p. 131]), and (vii) follows from (vi) because R^* is a nonabelian group with at most one involution. Since $|R^*| = n - 1$, (i) and (iii) imply (viii). (See also Hughes [4, p. 513].) Statements (ix), (x) are proved by Hughes [4, Theorem II.11], and (xi) follows from [6, Lemma 4.9] and a theorem of Hughes [2, p. 173, 12]. Finally, (xii) is proved in [7].

If a finite (V, OU), (U, OV) transitive plane π is of class $>$ I3 and if R^* is noncommutative, then π is either a "near-field plane" (of class IVa2 or IVa3), or a "dual near-field plane" (of class IVb2 or IVb3). In the former case π is (VU, VU) transitive and $(R, +)$ is associative. In the latter case π is (0, 0) transitive, so that the coordinatization is not the standard one; here $(R, +)$ has the right inverse property, but need not (and probably cannot) have the left inverse property.

Theorem A(vi) is proved by applying a certain homomorphism to the identity in Theorem A(v). It is suggested in Kantor [6] that some similar argument might be used to show that R^* cannot admit $C_p \times C_p$ as a homomorphic image, where C_p denotes a cyclic group of odd prime order p. This would be a major advance in the theory. Unfortunately the natural analogous procedure does not yield a result of such generality. However, we show in Theorem 1 and its corollary that the approach does furnish a weak numerical restriction, and that this has some modest application in excluding non-prime-power orders for class I3.

Theorem 1 *Let* π *be a plane of class at least* I3 *and of finite order* n. *Suppose that* R^* *admits* $C_p \times C_p$ *as a homomorphic image, where* C_p *is a group of odd prime order* p. *Then the Legendre symbol* $(q/p) = 1$ *for each odd prime* q *that divides the square-free part of* n. *Equivalently, there exist integers* x, y, z, *not all zero, such that*

$$nx^2 + (-1)^{(p-1)/2} py^2 = z^2.$$

Proof Let π be of class at least I3 and of finite order n, coordinatized as in Theorem A. Let $G = R^* \times R^*$, $D = \{(a, b) \in G \mid b = a + 1\}$, $G_1 = \{1\} \times R^*$, $G_2 = R^* \times \{1\}$, and $G_3 = \{(r, r) \mid r \in R^*\}$. Let $H = \langle\alpha\rangle \times \langle\beta\rangle$, where $\alpha^p = \beta^p = 1$ and $\alpha, \beta \neq 1$. Suppose that there exists an epimorphism $\phi\colon R^* \to H$, with kernel K. Let A, B be the complete inverse images in R^* of $\langle\beta\rangle$, $\langle\alpha\rangle$ respectively. Then there exist epimorphisms $\phi_1\colon R^* \to \langle\alpha\rangle$ and $\phi_2\colon R^* \to \langle\beta\rangle$, with kernels A and B, respectively. Define $\psi\colon G \to H$ by $\psi(r, s) = (\phi_1(r), \phi_2(s))$ for each $(r, s) \in G$. Then ψ is an epimorphism with kernel $A \times B$, and ψ can be extended to an epimorphism $\Psi\colon QG \to QH$, where QG, QH are the rational group algebras of G and H.

Let a_{ij} be the number of $d \in D$ such that $\psi(d) = \alpha^i\beta^j$, for $i, j = 0, 1, \ldots, p - 1$; then a_{ij} is also the number of $d \in D$ such that $\psi(d^{-1}) = \alpha^{-i}\beta^{-j}$. The restrictions of ψ to G_1, G_2 clearly have kernels of order $(n - 1)/p$, while the restriction of ψ to G_3 has kernel of order $(n - 1)/p^2$, because $A \cap B = K$. Hence, on applying Ψ to the identity in Theorem A(v), we find

$$\left(\sum_{i,j=0}^{p-1} a_{ij}\alpha^i\beta^j\right)\left(\sum_{k,m=0}^{p-1} a_{km}\alpha^{-k}\beta^{-m}\right) = n + (n-1)^2p^{-2}\sum_{i,j=0}^{p-1}\alpha^i\beta^j - (n-1)p^{-1}\sum_{j=0}^{p-1}\beta^j - (n-1)p^{-1}\sum_{i=0}^{p-1}\alpha^i - (n-1)p^{-2}\sum_{i,j=0}^{p-1}\alpha^i\beta^j. \tag{1}$$

It follows that

$$\left(\sum_{i,j=0}^{p-1} a_{ij}\alpha^i\beta^j\right)\left(\sum_{k,m=0}^{p-1} a_{km}\alpha^{-k}\beta^{-m}\right) = \sum_{r,s=0}^{p-1}\mu(r, s)\alpha^r\beta^s, \tag{2}$$

where

$$\begin{aligned}
&\mu(0, 0) = n + (n-1)^2p^{-2} - 2(n-1)p^{-1} - (n-1)p^{-2},\\
&\mu(0, t) = \mu(t, 0) = (n-1)^2p^{-2} - (n-1)p^{-1} - (n-1)p^{-2}\\
&\qquad\qquad \text{if} \quad t \neq 0,\\
&\mu(r, s) = (n-1)^2p^{-2} - (n-1)p^{-2} \qquad \text{if} \quad rs \neq 0.
\end{aligned} \tag{3}$$

Equating coefficients for the term $\alpha^r\beta^s$ in (2), we have

$$\mu(r, s) = \sum_{k,m=0}^{p-1} a_{k+r,m+s}a_{km} \qquad \text{for} \quad r, s = 0, 1, \ldots, p - 1, \tag{4}$$

where subscripts in (4) and hereafter are taken mod p.

Let $\nu(r, s) = \sum_{j=0}^{p-1}\mu(r + j, s + j)$, for $r, s = 0, 1, \ldots, p - 1$, and let

$Y_t = \sum_{i=0}^{p-1} a_{i,i+t}$ for $t = 0, 1, \ldots, p-1$. Then, by (4),

$$v(r,s) = \sum_{k,m=0}^{p-1} \left(\sum_{j=0}^{p-1} a_{k+r+j,\, s+m+j} \right) a_{km} = \sum_{k,m=0}^{p-1} Y_{s-r+k-m} a_{km}$$

$$= \sum_{k,t=0}^{p-1} Y_{s-r+t} a_{k,k+t}\,.$$

Hence

$$v(r,s) = \sum_{t=0}^{p-1} Y_{s-r+t} Y_t \tag{5}$$

Let M be the $p \times p$ symmetric circulant matrix with $M_{ij} = Y_{i+j-2}$, and let N be the $p \times p$ matrix with $N_{ij} = v(i,j)$, for $i, j = 0, 1, \ldots, p-1$. Then, by (5),

$$MM^{\mathrm{T}} = N. \tag{6}$$

On calculating the $v(i,j)$ from (3), we find $N = nI + (n-1)(n-4)p^{-1}J$, where I is the identity matrix and J is the matrix each of whose entries is one. Hence by Hughes [5, Lemma 3.1] N is positive definite, $\det N$ is the square of an integer, and for each odd prime q, the Hasse invariant $C_q(N) = (n,-1)_q^{(p-1)/2}(n,p)_q$, where $(a,b)_q$ denotes the Hilbert norm-residue symbol. It follows from the properties of this symbol (see, e.g., [2, p. 18]), and from the quadratic reciprocity theorem that $C_q(N) = (q/p)$ if q divides the square-free part of n and that $C_q(N) = 1$ otherwise. Now, by (6), the matrix N is rationally congruent to the identity matrix. By the Hasse–Minkowski theorem (Hasse [3]) this is possible only if $C_q(N) = 1$ for each odd prime q. Hence $(q/p) = 1$ for each odd prime q that divides the square-free part of n. Equivalently (cf. Hughes [5, Theorem 3.2]), the equation $nx^2 + (-1)^{(p-1)/2}py^2 = z^2$ has a nonzero solution in integers.

If n and p satisfy the conclusion of Theorem 1, the Minkowski–Hasse theorem ensures that there exists a rational matrix M that satisfies (6). One may still ask whether Eq. (1) has a solution in nonnegative integers. For $n = 28$ and $p = 3$ (which is the smallest case of interest in the context of Theorem 2 below), Eq. (1) has the solution $a_{00} = 2$, $a_{01} = 1$, $a_{02} = 5$, $a_{10} = 3$, $a_{11} = 4$, $a_{12} = 2$, $a_{20} = 3$, $a_{21} = 4$, $a_{22} = 2$.

The conclusion of Theorem 1 is always satisfied if n is a prime power and p divides $n-1$. When n is even, Theorem 1 gives less information than Theorem A(iv), and when $n \equiv 1$ or $2 \pmod 4$, the values of n to which Theorem 1 can be applied may well be excluded by the Bruck–Ryser theorem [2, p. 144, 13]. However, Theorem 1 does imply the nonexistence of planes of class I3 with order n for infinitely many $n \equiv 3 \pmod 4$ that are not otherwise excluded.

Corollary (a) *There is no plane of class* I3 *with order* $n = 1 + 2p^r$, *where* p *is an odd prime, if the square-free part of* n *is divisible by a prime* q *such that* $(q/p) = -1$.

(b) *There is no plane of class* I3 *with order* $n = 1 + 2p^r$ *if* p *is a prime* $\equiv$ 7 (mod 12) *and if* $r(p-1)/3 \not\equiv 1 \pmod 3$.

Proof (a) If π is of class I3 with order $n = 1 + 2p^r$, then $|R^*| = 2p^r$. By Theorem A(ii), $R^* = \langle\sigma\rangle \times T$, where σ is the unique involution in R^* and T is the Sylow p-group of R^*. Since R^* is nonabelian, T is nonabelian, whence $r \geqslant 3$. It follows that T, hence also R^*, admits $C_p \times C_p$ as a homomorphic image (as is easily shown by induction on r). Now apply Theorem 1.

(b) Suppose that $p \equiv 7 \pmod{12}$ and that $r(p-1)/3 \not\equiv 1 \pmod 3$. Then 3 divides n, but 3^2 does not because $1 + 2p^r = 1 + 2[1 + (p-1)]^r \equiv 3 + 2r(p-1) \pmod{3^2}$. Since $p \equiv 3 \pmod 4$, the quadratic reciprocity theorem ensures that $(3/p) = -(p/3) = -1$.

As was noted some time ago in Yaqub [11], it is not hard to show that most non-prime-powers $\leqslant 100$ cannot be the order of a plane of class I3. In Theorem 2 we list all orders $n \leqslant 250$ that cannot yet be excluded. Non-prime-powers are in bold-faced type, and values n for which there exists a (genuine) near-field of order n carry an asterisk; the remaining values are primes, except for $125 = 5^3$, for which no near-field exists. (See, e.g., [2, pp. 228–231].)

Theorem 2 *If there exists a plane of class* I3 *with order* $n \leqslant 250$, *then* $n =$ 13, 25*, **28**, 29, 37, 41, 43, **45**, 49*, 53, 61, 64*, 73, **76**, 79, 81*, **85**, 89, 97, 101, 109, **111**, **112**, 113, **115**, **117**, 121*, 125, 127, 137, **145**, **148**, 149, 151, **153**, 163, 169*, **172**, 173, **185**, **187**, 193, **196**, **205**, 211, **221**, 223, **225**, 229, 233, **235**, 241, **244**, *or* **245**.

Proof The values $n =$ 40, 56, 58, 82, 130, 156, 184, 202, 204, 220, 226, 232, 248 are excluded by Theorem A(iv), the values $n =$ 17, 65 by Theorem A(vi), and the value $n = 55$ by the corollary to Theorem 1. All other values except $n = 9$ are excluded either by the Bruck–Ryser theorem or by the fact that every group of order $n - 1$ that contains at most one involution is abelian.

Suppose $n = 9$. Then, by Theorem A(iii), R^* is the quaternion group $\langle a, b \mid a^4 = b^4 = 1, a^2 = b^2, b^{-1}ab = a^{-1}\rangle$. Let z denote the unique involution in R^*. (Note that we cannot assume $z = -1$.) Then $R^* = \{1, z, a, b, za, zb, ab, ba\}$. The group Aut R^* is transitive on the elements of order 4, and the subgroup that fixes a is transitive on $R^* - \langle a\rangle$. We construct all nonisomorphic loops $(R, +)$ that are compatible with the distributive law, by considering the successive possibilities for $1 + x$ as x runs through R^*. Whenever possible, we use the existence of automorphisms of R^* to reduce the number of cases. Thus, for example, if $1 + 1$ is of order 4, we may assume without loss of generality that $1 + 1 = a$. Then $1 + z \neq 1$ or z, and $1 + z \neq za$ because $z + z = za$; hence we can assume that $1 + z = 0$ or b. In this way we

find only the following six loops:

(i) $1+1=0$, $1+z=a$, $1+a=b$, $1+b=z$, $1+za=ab$, $1+zb=za$, $1+ab=ba$, $1+ba=zb$.

(ii) $1+1=0$, $1+z=a$, $1+a=b$, $1+b=zb$, $1+za=ba$, $1+zb=ab$, $1+ab=z$, $1+ba=za$.

(iii) $1+1=z$, $1+z=0$, $1+a=b$, $1+b=a$, $1+za=ba$, $1+zb=ab$, $1+ab=zb$, $1+ba=za$.

(iv) $1+1=z$, $1+z=0$, $1+a=b$, $1+b=ba$, $1+za=ab$, $1+zb=za$, $1+ab=zb$, $1+ba=a$.

(v) $1+1=z$, $1+z=0$, $1+a=b$, $1+b=ab$, $1+za=ba$, $1+zb=za$, $1+ab=a$, $1+ba=zb$.

(vi) $1+1=z$, $1+z=0$, $1+a=b$, $1+b=a$, $1+za=ab$, $1+zb=ba$, $1+ab=za$, $1+ba=zb$.

The first four loops are nonplanar; this can easily be verified by finding $r, x, y \in R$ with $r \neq 1$, $x \neq y$, and $(r+x)^{-1}(1+x) = (r+y)^{-1}(1+y)$. (See, e.g., Yaqub [10, p. 377].) It follows that loops (v) and (vi) must correspond to the near-field plane of order 9 and its dual (of class IVa3 and class IVb3, respectively) since these planes must appear as solutions. Hence there is no plane of class I3 with order 9.

Henceforth we shall assume that $(R, +)$ has both inverse properties. Then Theorem B applies, and in particular $(R, +)$ is commutative. The following lemma is essentially contained in Kantor [7], but we include the proof because cases (ii) and (iv) of part (b) do not arise there. (See also the proof of Hughes [4, Theorem II.11].)

Lemma *Suppose that π is finite, of class at least* I3, *and that $(R, +)$ has both inverse properties. Suppose also that $a, b \in R^*$ and that $a + b = -1$. Let Σ be the set consisting of the distinct elements from among $a, a^{-1}, b, b^{-1}, a^{-1}b, b^{-1}a$. Then:*

(a) $a^{-1} + a^{-1}b = -1 = b^{-1} + b^{-1}a$.

(b) *Either* (i) $|\Sigma| = 6$, *or* (ii) $\Sigma = \{c, c^{-1}\}$ *where* $c \neq 1$, $c^3 = 1$, *and* $c + c^{-1} = -1$, *or* (iii) $\Sigma = \{1\}$ *and* $1 + 1 = -1$, *or* (iv) $\Sigma = \{1, c, c^{-1}\}$ *where* $c \neq 1, -1$ *and* $1 + c = -1 = c^{-1} + c^{-1}$.

(c) $R^* - \{-1\}$ *can be partitioned into sets of type* (i)–(iv). *If a is of order* 3, *then a belongs to a set of type* (ii). *There is at most one set of type* (iv).

(d) *If N is a subgroup of index* 2 *in R^*, and if Σ is a member of the partition such that $|\Sigma| = 6$, then $|N \cap \Sigma| = 2$ or* 6.

Proof (a) If $a, b \in R^*$ and if $a + b = -1$, then $a \neq -1 \neq b$. By Theorem B(i), $(-1)^2 = 1$ and $x(-1) = (-1)x$ for all $x \in R^*$. Thus $a + b = -1 \Rightarrow a = -1 + (-1)b$, by the inverse property, $\Rightarrow -1 = a^{-1} + a^{-1}b$ by the distributive law. Similarly, $b^{-1} + b^{-1}a = -1$.

(b) Suppose that $|\Sigma| < 6$. Then, without loss of generality, we may assume that $a = a^{-1}$, b, b^{-1}, $a^{-1}b$, or $b^{-1}a$. If $a = a^{-1}$, then $a = 1$ since $a \neq -1$; similarly, if $a = b^{-1}a$, then $b = 1$. Now if $a = b = 1$, then Σ is of type (iii), and if $a = 1 \neq b$ (or if $b = 1 \neq a$), then Σ is of type (iv), with $c = b$ ($c = a$, respectively). Again, if $a = b \neq 1$, then Σ is of type (iv), with $c = a^{-1}$. Suppose next that $a = b^{-1}$, with $a \neq 1$. Then $a + a^{-1} = -1 \Rightarrow a^2 = (-1) \times (1 + a) \Rightarrow 1 + a = (-1)a^2$. Hence a is of order 3, by Theorem B(iv), and Σ is of type (ii). Suppose finally that $a = a^{-1}b$ with $a \neq 1$. Then $a + a^2 = -1$, so that again $1 + a = (-1)a^2$ and Σ is of type (ii).

(c) Clearly, $R^* - \{-1\}$ can be partitioned into sets Σ of type (i)–(iv). If a is of order 3, then $a + a^{-1} = -1$ by Theorem B(iv), whence a belongs to a set of type (ii). If Σ is of type (iv), then $c = (-1)(1 + 1)$. Hence there is at most one such set.

(d) Suppose $|\Sigma| = 6$ and that N is of index 2 in R^*. If $a, b \in N$, then $|N \cap \Sigma| = 6$. Otherwise, $|N \cap \Sigma| = 2$ because N is of index 2.

We shall call the above sets of type (i)–(iv) "Σ-sets"; a Σ-set is "proper" if and only if $|\Sigma| = 6$.

Theorem 3 *Suppose that π is of class* I3 *with order n, and that $(R, +)$ has both inverse properties.*

(i) *If $1 + 1$ is of order 4, then π contains a subplane of order 5.*

(ii) *If $1 + 1$ is of order 3, then π contains a subplane of order 7.*

(iii) *$1 + 1$ is not of order 6.*

(iv) *If $n - 1 = 4p$, where p is a prime ≥ 3, then $1 + 1$ is of order 4.*

(v) *If p is a prime > 3, then $n - 1 \neq 6p$.*

(vi) *If n is even and if $R^* = \langle a, N \rangle$, where $a^3 = 1$ and N is a normal subgroup of index 3 in R^*, then a cannot act fixed point free on N.*

(vii) *If p is a prime > 3, then $n - 1 \neq 3p$.*

(viii) *If p is an odd prime $\equiv -1 \pmod 3$, then $n - 1 \neq 3p^2$.*

Proof (i) Suppose that $1 + 1 = a$, where a has order 4. Then n is odd, and $a^2 = -1, \neq 1$ by Theorem B(viii). Using the inverse properties and the commutativity of $(R, +)$, we find $1 + a = a^{-1}$ and $1 + a^{-1} = -1$. Hence the set $\{0\} \cup \langle a \rangle$ is closed under addition and multiplication, and must therefore coordinatize a subplane of order 5.

(ii) Suppose that $1 + 1 = b$, where b has order 3. Then n is odd and $-1 \neq 1$. Let $a = (-1)b$, so that a has order 6 and $b = a^4$. By Theorem B(iv) $1 + a^4 = a^5$ and $1 + a^2 = a$. Also, since $1 + 1 = a^4$, we have $1 = a^4 - 1 = a^4 + a^3$, whence $1 + a = a^3$ and $1 + a^5 = a^2$. Hence $\{0\} \cup \langle a \rangle$ is closed under addition and multiplication, and must coordinatize a subplane of order 7.

(iii) Suppose that $1 + 1 = a$, where a has order 6. Then n is odd, and

$a = (-1)b$, where b has order 3. But then, by Theorem B(iv), $1 + b^{-1} = (-1)b$, a contradiction since $b \neq 1$.

(iv) Suppose that $n - 1 = 4p$, where p is a prime $\geqslant 3$. Then, since R^* is nonabelian and contains a unique involution, $R^* = \langle a, b \mid a^4 = 1 = b^p, a^{-1}ba = b^{-1}\rangle$. The subgroup $N = \langle a^2, b\rangle$ is of index 2 in R^*, and $R^* - N$ consists of all elements of R^* that have order 4. If Σ is a proper Σ-set, then by the lemma, $|\Sigma \cap (R^* - N)| = 0$ or 4. Since $|R^* - N| = 2p \equiv 2 \pmod 4$, it follows that there exist elements c, c^{-1} of order 4 which belong to a Σ-set Σ_1 that is not proper. Clearly, Σ_1 is of type (iv). Hence $1 + 1$ is of order 4.

(v) Suppose $n - 1 = 6p$, where p is a prime > 3. Since R^* contains the unique involution -1 and since $3p$ is odd, $R^* = \langle -1\rangle \times S$ with $|S| = 3p$. Since $p > 3$, the Sylow p-group of S is normal, and since R^* is nonabelian, it follows that $p \equiv 1 \pmod 3$ and that S has p Sylow 3-groups. Hence S contains p Σ-sets of type (ii). Let n_1, n_2 be the numbers of elements in S, $R^* < S$, respectively, which are contained in proper Σ-sets. If $1 + 1 = -1$, then $n_1 = p - 1$ and $n_2 = 3p - 1$ since $R^* - S$ contains no element of order 3. If $(-1)(1 + 1) = c \neq 1$, then $n_1 = p - 3$ and $n_2 = 3p - 1$ if $c \in S$, while $n_1 = p - 1$ and $n_2 = 3p - 3$ if $c \notin S$. Hence $n_1 \leqslant p - 1$ and $n_2 \geqslant 3p - 3$. But, by the lemma, if Σ is a proper Σ-set such that $|\Sigma \cap (R^* - S)| > 0$, then Σ contains four elements of $R^* - S$ and two elements of S. Hence $n_2 \leqslant 2n_1$. This yields the contradiction $3p - 3 \leqslant 2(p - 1)$.

(vi) Suppose that n is even and that $R^* = \langle a, N\rangle$ where $a^3 = 1$ and N is a normal subgroup of index 3 in R^*. We can assume that $|N| > 1$, since otherwise π is of order 4, hence desarguesian. Suppose that a acts fixed point free on N, i.e., that $a^{-1}xa = x$ with $x \in N$ implies $x = 1$. Then $|N| \equiv 1 \pmod 3$, and $\langle a\rangle$ is a Sylow 3-group of R^*. Now $xax^{-1} = a$ with $x \in N$ implies $x = 1$, and $xax^{-1} = a^{-1}$ implies $x^2ax^{-2} = a$, whence $x = 1$ because n is even. Hence R^* contains $|N|$ Sylow 3-groups, and every element of R^* either belongs to N or has order 3. By Theorem B(iv) if c is of order 3, then $1 + c = c^{-1}$ since here $-1 = 1$. It follows that if $x \in N$, $x \neq 1$, then $1 + x \in N$. Thus, again because $1 + 1 = 0$, the set $\{0\} \cup N$ is closed under addition and multiplication, and must therefore coordinatize a subplane of order $1 + |N|$. By Bruck's theorem [2, p. 145, 18], this implies that $(1 + |N|)^2 \leqslant 1 + 3|N|$, i.e., that $|N| = 1$, a contradiction.

(vii) Suppose p is a prime > 3. If $n - 1 = 3p$, the Sylow p-group N of R^* is normal and of index 3, and $R^* = \langle a, N\rangle$ where a is any element of order 3. Since $|N| = p$ and since a cannot act fixed point free on N by (vi), R^* is abelian.

(viii) Suppose $p \equiv -1 \pmod 3$ and that $n - 1 = 3p^2$. Again, the Sylow p-group N of R^* is normal and of index 3, and $R^* = \langle a, N\rangle$ where a has order 3. The centralizer of a in N is nontrivial by (vi), and cannot be of order p since then a would act fixed point free on the $p^2 - p$ remaining elements of

N, where $p^2 - p \equiv 2 \pmod 3$. Hence a centralizes N, and, since N is abelian, R^* is abelian.

Theorem 4 *There is no plane π of class* I3 *and of order n such that $(R, +)$ has both inverse properties for the following values of $n \leqslant 250$: $n =$* 13, 25*, **28**, 29, 43, **45**, **76**, 79, **111**, **112**, **115**, **117**, 163, **187**, 223, **244**.

Proof The values $n = 45, 111, 117$ are excluded by Theorem B(xii), and the values $n = 28, 163, 244$ by Theorem B(vii). If $n = 43, 79, 115, 187$, or 223 we can apply Theorem 3(v). If $n = 13$ or 29, then by Theorem 3(iv) and (i), π contains a subplane of order 5; in each case this contradicts Bruck's theorem. The values $n = 76, 112$ are excluded by Theorem 3(viii), (vii), respectively. Thus it remains to be shown that $n \neq 25$.

If $n = 25$, then, since R^* contains a unique involution, there are four nonisomorphic possibilities for R^* [1, §126]. These are:

(i) $\langle a, b, c \mid a^4 = b^4 = 1,\ a^2 = b^2,\ b^{-1}ab = a^{-1},\ c^3 = 1,\ a^{-1}ca = c,\ b^{-1}cb = c\rangle$,

(ii) $\langle a, b, c \mid a^4 = b^4 = 1,\ a^2 = b^2,\ b^{-1}ab = a^{-1},\ c^3 = 1,\ a^{-1}ca = c,\ b^{-1}cb = c^{-1}\rangle$,

(iii) $\langle a, b, c \mid a^4 = b^4 = 1,\ a^2 = b^2,\ b^{-1}ab = a^{-1},\ c^3 = 1,\ c^{-1}ac = b,\ c^{-1}bc = ab\rangle$,

(iv) $\langle a, b \mid a^8 = 1 = b^3,\ a^{-1}ba = b^{-1}\rangle$.

We note that the regular and irregular near-fields of order 25 have multiplicative groups of type (iv) and (iii), respectively.

Suppose first that R^* is of type (i) or (ii). Then, in each case, R^* contains exactly two elements of order 3, namely c and c^{-1}, and the group $N_1 = \langle a, c\rangle$ is of index 2 in R^*. Since $|R^* - N_1| = 12 \equiv 0 \pmod 4$, and since $1, -1, c, c^{-1} \in N$, it follows from the lemma that each Σ-set that contains an element of $R^* - N_1$ is proper; there are three such sets, each containing two elements of N_1. The remaining six elements of N_1 include 1, -1, c, and c^{-1}. Since $\{c, c^{-1}\}$ is a Σ-set of type (ii), we cannot have $1 + 1 = -1$. Hence N_1 contains a Σ-set of type (iv), say $\{1, d, d^{-1}\}$, with $1 + d = -1$, where also $1 + 1 = (-1)d$. Now $N_2 = \langle b, c\rangle$ is also of index 2 in R^* for both types, and the same argument shows that $\{1, d, d^{-1}\} \subset N_2$. Since $N_1 \cap N_2 = \langle -1\rangle \times \langle c\rangle$, the element d is of order 3 or 6, whence $1 + 1$ is of order 6 or 3. By Theorem 3(iii), $1 + 1$ is not of order 6. If $1 + 1$ is of order 3, then by Theorem 3(ii), π contains a subplane of order 7; this contradicts Bruck's theorem. Hence R^* is not of type (i) or (ii).

Suppose next that R^* is of type (iii). Write $z = a^2 = b^2 = -1$. Then, besides 1 and z, R^* contains six elements of order 4, eight elements of order 3, and eight elements of order 6. The elements of order 3 form four Σ-sets of type (ii), and it follows from the lemma that there exists a Σ-set $\{1, d, d^{-1}\}$ of

type (iv), with $1 + 1 = zd$. As has just been shown, d cannot be of order 3 or 6. Hence $1 + 1$ is of order 4, and we can assume without loss of generality that $1 + 1 = a$. We are left with four elements of order 4 and eight elements of order 6 with which to construct two proper Σ-sets, say Σ_1 and Σ_2. The elements of order 4 cannot all be in the same Σ-set. So suppose that $b, b^{-1} \in \Sigma_1$ and that $ab, a^{-1}b \in \Sigma_2$. Then there exists an element x of order 6 such that $b + x = z$. If $x = zc$, then $b^{-1} + b^{-1}zc = z$, i.e., $b^{-1} + bc = z$, and this is impossible because bc has order 3. Similarly, we find that $x \neq bc^{-1}, a^{-1}bc, abc^{-1}$. Hence either (1) $b + zc^{-1} = z$, (2) $b + ac^{-1} = z$, (3) $b + b^{-1}c = z$, or (4) $b + a^{-1}c = z$.

In case (1), $\Sigma_1 = \{b, b^{-1}, zc^{-1}, zc, bc^{-1}, a^{-1}c\}$, whence $\Sigma_2 = \{ab, a^{-1}b, ac^{-1}, b^{-1}c, a^{-1}bc, abc^{-1}\}$. There exists an element $y \in \Sigma_2$ such that y has order 6 and $ab + y = z$. If $y = ac^{-1}$, then $1 + b^{-1}c^{-1} = b^{-1}a^{-1}z$, which contradicts the fact that $b^{-1}c^{-1}$ has order 3. Similarly, $y \neq abc^{-1}$. If $y = a^{-1}bc$, then $1 + zc = b^{-1}a^{-1}z$. But $b + zc^{-1} = z \Rightarrow z + c^{-1} = b \Rightarrow zc + 1 = cb$. This is a contradiction, since $b^{-1}a^{-1}z \neq cb$. Similarly, $y \neq b^{-1}c$. Hence case (1) cannot occur. The same kind of calculations show that case (2) cannot occur, and that in case (3) the only possibility is $ab + bc^{-1} = z$. The loop obtained in case (3) is not planar since, for example, $(1 + b)^{-1}(a + b) = a^{-1}bc = (1 + a^{-1}c^{-1})^{-1}(a + a^{-1}c^{-1})$. Finally, in case (4), we find that the only possibility is $ab + zc^{-1} = z$; this must yield the plane of class IVa2 over the irregular near-field of order 25 since this plane must appear as a solution. Hence there is no plane of class I3 with R^* of type (iii).

Suppose, finally, that R^* is of type (iv). Write $a^4 = z = -1$. Then, in addition to 1 and z, R^* contains two elements of order 3, two elements of order 6, four elements of order 12, and 12 elements of order 8. Let $N = \langle a^2, b\rangle$; then N is of index 2 in R^* and all elements of $R^* - N$ are of order 8. By the lemma, since $|R^* - N| = 12$, the element $1 + 1$ must belong to N, and there are three proper Σ-sets that contain elements of $R^* - N$. Since these use altogether six elements of N, and since $\{b, b^{-1}\} \subset N$ is the only Σ-set of type (ii), there exists a Σ-set $\{1, d, d^{-1}\} \subset N$ of type (iv), with $1 + 1 = zd$. It was shown earlier that d cannot be of order 3 or 6. Hence d has order 12 or 4. If d has order 12, there exists a Σ-set Σ that contains four elements of order 8 and the two elements of order 4. Moreover, there exist $x, y \in \Sigma$ such that x, y have order 8, $x + y = z$ and $x^{-1}y$ has order 4. It follows that $y = x^{-1}$ or x^3. Since $x + x^{-1} = z$ only if $x^3 = 1$, we must have $x + x^3 = z$. Then $1 + x^2 = x^{-1}z = x^3$. Let $1 + 1 = t$, so that $t = zd$ has order 12. Then $x^2 + x^2 = x^2t$. By planarity, $(x^2 + 1)^{-1}(1 + 1) \neq (x^2 + x^2)^{-1}(1 + x^2)$, i.e., $x^5t \neq t^{-1}x$. But, since t has order 12, $t = x_1b_1 = b_1x_1$ where $x_1 = x^2$ or x^6 and $b_1 = b$ or b^{-1}. Thus $x^5t = zxx_1b_1$ and $t^{-1}x = x_1^{-1}b_1^{-1}x = x_1^{-1}xb_1 = zxx_1b_1$. Hence $1 + 1$ is not of order 12.

We can now assume that $1 + 1$ is of order 4. In this case there exists a proper Σ-set Σ_1 that contains four elements of order 8 and the two elements of order 6. Since Aut R^* is transitive on the elements of order 8 and on the elements of order 3, we can assume without loss of generality that $a, zb \in \Sigma_1$ and that $a + zb = z$. Then $\Sigma_1 = \{a, a^{-1}, zb, zb^{-1}, a^3b, a^5b\}$. (Note that we do not specify at this stage whether $1 + 1 = a^2$ or a^6 since this would distinguish between a and a^{-1} in $(R, +)$.) There are two other proper Σ-sets, Σ_2 and Σ_3, each of which contains four elements of order 8 and two elements of order 12. Since neither Σ_2 nor Σ_3 can contain four elements from the same Sylow 2-group of R^*, we can assume that $a^3, a^5, a^2b^{-1}, a^6b^{-1} \in \Sigma_2$. Then either (1) $a^3b^{-1}, a^5b^{-1} \in \Sigma_2$ or (2) $ab^{-1}, a^{-1}b^{-1} \in \Sigma_2$.

In case (1) we have either (i) $a^3 + a^5b^{-1} = z$ or (ii) $a^5 + a^3b^{-1} = z$ (since $a^2b^{-1}, a^6b^{-1} \in \Sigma_2$). Furthermore, $\Sigma_3 = \{ab^{-1}, a^{-1}b^{-1}, ab, a^{-1}b, a^2b, a^6b\}$, where either (iii) $ab^{-1} + a^{-1}b = z$ or (iv) $a^{-1}b^{-1} + ab = z$. Now (i) and (iv) are incompatible since (i) implies $1 + a^5 = a^6b^{-1}$, while (iv) implies $1 + ab^{-1} = a^6b^{-1}$. Similarly, (ii) and (iii) are incompatible since (ii) implies $1 + a^3 = a^2b^{-1}$, while (iii) implies $1 + a^{-1}b^{-1} = a^2b^{-1}$. If (i) and (iii) hold, we find $(a^2 + a^{-1})^{-1}(1 + a^{-1}) = a^{-1} = (a^2 + ab)^{-1}(1 + ab)$; if (ii) and (iv) hold, then $(a^2 + a^5)^{-1}(1 + a^5) = a^3b = (a^2 + a^2b)^{-1}(1 + a^2b)$. Thus the loops obtained from case (1) are nonplanar.

In case (2) we find by considering Σ_2 that either (v) $a^3 + ab^{-1} = z$ or (vi) $a^5 + a^{-1}b^{-1} = z$, and by considering Σ_3 that either (vii) $ab + a^3b^{-1} = z$ or (viii) $a^{-1}b + a^5b^{-1} = z$. Here it turns out that (v) and (vii) are incompatible, as also are (vi) and (viii). If (v) and (viii) hold, then $(a^2 + a^3) \times {}^{-1}(1 + a^3) = a^3 = (a^2 + a^5b^{-1})^{-1}(1 + a^5b^{-1})$, and no plane is obtained. So suppose that (vi) and (vii) hold. In order to determine the complete loop $(R, +)$, we must define either $1 + 1 = a^2$ or $1 + 1 = a^6$. But if $1 + 1 = a^2$, then $(a + a^{-1})^{-1}(1 + a^{-1}) = a^2b = (a + b^{-1})^{-1}(1 + b^{-1})$. Hence, to within isomorphism, there exists only one planar loop $(R, +)$ that is compatible with R^*, and this must yield the plane of class IVa2 over the regular near-field of order 25. This completes the proof that there is no plane of class I3 and of order 25 that satisfies the hypotheses of Theorem 4.

By Theorems 2 and 4, there are only 12 nonprime powers ≤ 250 that are still "possible" orders for a plane that satisfies the conditions of Theorem 4; the three smallest of these are 85, 145, and 148. It is perhaps more significant that there is no plane of this kind with order 25. However, for $n = p^2$, where p is a prime > 3, it may well make a difference whether $p \equiv 1$ or $3 \pmod 4$ (since this determines whether the Sylow 2-groups of R^* are cyclic or generalized quaternion for the regular near-field), and whether $p \equiv 1$ or $2 \pmod 3$ (since the elements of order 3 clearly play an important role in limiting the possible Σ-sets). On both counts, and for other obvious reasons, the case

$n = 49$ is of particular interest; however, it is probably too large to handle by the methods used here. In principle, the question of the existence of planes of class I3 with "small" order could be settled by computer (cf. Pankin [8]). The assumption that $(R, +)$ has both inverse properties reduces the number of additive loops substantially. (Even $n = 13$ would be very laborious to decide by hand in the general case.) However, there is no reason to suppose that finite planes of class I3 must satisfy the assumption.

REFERENCES

[1] W. Burnside, "Theory of Groups of Finite Order," 2nd ed. Dover, New York, 1955.
[2] P. Dembowski, "Finite Geometries." Springer-Verlag, Berlin and New York, 1968.
[3] H. Hasse, Über die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen, *J. Reine Angew. Math.* **152** (1923), 205–224.
[4] D. R. Hughes, Planar division neo-rings, *Trans. Amer. Math. Soc.* **80** (1955), 502–527.
[5] D. R. Hughes, Collineations and generalized incidence matrices, *Trans. Amer. Math. Soc.* **86** (1957), 284–296.
[6] W. M. Kantor, Projective planes of type I4, *Geometriae Dedicata* **3** (1974), 335–346.
[7] W. M. Kantor, Projective planes of type I4: Addendum, *Geometriae Dedicata*, to appear.
[8] M. Pankin, Finite planes of type I4, *Proc. Intl. Conf. Proj. Planes*, pp. 215–218. Washington State Univ. Press, 1973.
[9] G. Pickert, "Projektive Ebenen," 2nd ed. Springer-Verlag, Berlin and New York, 1975.
[10] J. Yaqub, The existence of projective planes of class I3, *Arch. Math. (Basel)* **12** (1961), 374–381.
[11] J. Yaqub, The Lenz–Barlotti classification, *Proc. Proj. Geometry Conf.*, pp. 129–160. Univ. of Illinois at Chicago, 1967.

AMOS (MOS) 1970 subject classification: 50A20.

A Theorem on Cyclic Algebras

HANS ZASSENHAUS

THE OHIO STATE UNIVERSITY
COLUMBUS, OHIO

Introduction

A *cyclic algebra* was defined by L. E. Dickson as a hypercomplex system H generated by two elements a, b over a field F such that:

(1) the subalgebra of H generated by a alone is a cyclic extension E of finite degree n over F where the automorphism group of E over F is generated by a certain automorphism σ of order n;
(2) b is invertible and

$$b^{-1}ab = a\sigma. \tag{1}$$

Olga Taussky studied in [2–4] the question of what one can say about the reduced norm of the commutator

$$c = [\hat{a}, \hat{b}] = \hat{a}\hat{b} - \hat{b}\hat{a} \qquad (\hat{a} \in F(a), \quad \hat{b} \in F(a) + F(a)H) \tag{2}$$

in the case that $n = 2$ and H is a matrix algebra over F. By her results she established an interesting relation between the multiplicative commutator

equation

$$(a, b) = a^{-1}b^{-1}ab = a^{-1}(a\sigma) \tag{3a}$$

and the little studied additive commutator equation motivating the present investigation.

Let us mention right away that for arbitrary $\hat{a}$, a_1, a_2 of $F(a)$ and elements $a_1 + ba_2$ of $F(a) + bF(a)$ there holds the commutator equation

$$[\hat{a}, b] = ba_2(\hat{a}\sigma - \hat{a}) \tag{3b}$$

where the elements on the right-hand side of (3a) are characterized as the elements of E of norm 1 according to Hilbert Satz 90, whereas the elements $\hat{a}\sigma - \hat{a}$ occurring on the right of (3b) of the additive version are characterized as the trace zero elements of E.

1. Simple Properties of Cyclic Algebras

It follows from the definition of a cyclic algebra H that H is a centrally simple associative algebra with the n^2 basis elements a^ib^k $(0 \leq i < n, 0 \leq k < n)$, that

$$0 \neq b^n = \beta \in F \tag{4}$$

and that β is uniquely determined by H and the structure of E over F modulo the norm group $N_{E/F}(E\backslash 0)$, the multiplicative group formed by all nonzero elements of F that are norms of some element of E over F.

The algebra H is a ring of matrices of degree n over F precisely if β is in the norm group.

Indeed, if a satisfies the irreducible equation $f(a) = 0$ where

$$f(t) = t^n - \alpha_1 t^{n-1} + \cdots + (-1)^n\alpha_n \qquad (\alpha_i \in F, \quad 1 \leq i \leq n) \tag{5}$$

is some irreducible polynomial of degree n over F and if

$$a^{i-1}\sigma = \sum_{k=1}^{n} \beta_{ik}a^{k-1} \qquad (\beta_{ik} \in F, \quad 1 \leq i \leq n, \quad 1 \leq k \leq n), \tag{6}$$

then the companion matrix

$$a = \begin{bmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & & \ddots \\ & & & 1 \\ (-1)^{n-1}\alpha_n & & \cdots & \alpha_1 \end{bmatrix}$$

and the matrix $b = (\beta_{ik})$ generate the full matrix algebra of degree n over F presented as a cyclic algebra such that $\beta = 1$, unique up to a norm factor.

In general there is the split model of H generated by the two matrices

$$a = \begin{bmatrix} \alpha\sigma & & & \\ & \alpha\sigma^2 & & \\ & & \ddots & \\ & & & \alpha\sigma^n \end{bmatrix}, \qquad b = \begin{bmatrix} \beta_1 & & & \\ 0 & \beta_2 & & \\ & 0 & \ddots & \\ & & \ddots & \beta_{n-1} \\ \beta_n & 0 & \cdots & 0 \end{bmatrix}$$

with coefficients $\alpha, \alpha\sigma, \ldots, \alpha\sigma^{n-1}, \beta_1, \ldots, \beta_n$ in some splitting extension Φ of f over F such that

$$f(t) = \prod_{j=1}^{n} (t - a\sigma^{j-1}) \tag{7a}$$

$$\beta = \beta_1 \beta_2 \cdots \beta_n , \tag{7b}$$

which gives a concrete model of the cyclic algebra H over F.

As is well known, any finite-dimensional centrally simple associative algebra H over the field F contains maximal commutative subalgebras that are finite separable extensions of F. In particular, if H is of dimension 4 over F, then H contains a separable quadratic extension E of F. This means that in the latter case E is a cyclic extension with involutory generating automorphism σ over F such that there is some invertible element b of H so that for any generator a of E over F we have (1) and H is cyclic.

On the other hand, it has been shown recently that not every centrally simple hypercomplex system is a cyclic algebra.

We observe that

$$H = \sum_{k=0}^{n-1} \cdot b^k E \tag{8a}$$

and according to (1)

$$ab^k - b^k a\sigma^k = 0 \tag{8b}$$

so that

$$[b^k, a] = b^k a - ab^k = b^k(a - a\sigma^k) \tag{8c}$$

$$[E + b^k E] = b^k \ker \mathrm{tr} \qquad (k \in \mathbb{Z}, \quad \gcd(k, n) = 1) \tag{8d}$$

where tr is the F-linear trace mapping

$$E \to F\colon \mathrm{tr}$$

$$x\,\mathrm{tr} = \sum_{j=0}^{n-1} x\sigma^j \qquad (\chi \in E)$$

of E on F. Note that the well-known additive version of Hilbert Satz 90 just

tells us that

$$E(1-\sigma) = \ker \mathrm{tr}. \tag{8e}$$

In the event that the degree n of E over F is not divisible by the characteristic of F a considerable simplification of the problem is achieved by adjoining to the field of reference F a primitive nth root of unity ζ such that over the new field of reference $F_1 = F(\zeta)$ there arises the generalized cyclic algebra $H_1 = F_1 \otimes_F H = F_1 H$ containing the separable normal commutative algebra $E_1 = F_1 \otimes_F E = F_1 E = F_1(a)$ of dimension n over F_1 with generating automorphism

$$E_1 \to E_1 \colon \sigma_1$$

$$(\alpha \underset{F}{\otimes} \eta)\sigma_1 = \alpha \underset{F}{\otimes} (\eta\sigma) \qquad (\alpha \in F_1, \quad \eta \in E)$$

and with standard generators a, b.

The simplification is achieved by Lagrange's construction according to which

$$E_1 = F_1(a_1),\ 0 \neq a_1^n = \alpha \in F_1,\ |\alpha/(F_1 \setminus 0)^n| = n, \tag{9}$$

$$a_1 \sigma_1 = \zeta a_1 \tag{10}$$

and Eq. (9) assumes the form

$$b^{-1} a_1 b = \zeta a_1 \tag{11}$$

or, without inversion,

$$a_1 b - \zeta b a_1 = 0. \tag{12}$$

The latter form of condition (11) has the virtue that for given a_1 the equation

$$a_1 x - \zeta x a_1 = 0 \tag{13}$$

defines the n-dimensional linear solution space $E_1 b = bE_1$.

Any one of its regular elements together with any generator of E_1 over F presents H_1 as a cyclic algebra.

2. A Theorem on Cyclic Algebras

Generalizing a recent theorem of O. Taussky for $n = 2$, we have

Theorem 1 (a) *For given $\hat{a}$ of E the norms of the Lie products*

$$[x, \hat{a}] \qquad (x \in E + bE)$$

over F form the set

$$\zeta^{\binom{n}{2}}\beta N(F)$$

where ζ is a primitive nth root of unity.

(b) *The norms of the Lie products*

$$[\hat{b}, E]$$

($\hat{b}$ a fixed regular element of $E + bE$) over F run through all of

$$\zeta^{\binom{n}{2}}\beta N(F).$$

(c) *For any order Λ of H over the integral domain $\Lambda \cap F$ with quotient field F and for given $\hat{a}$ of $\Lambda \cap E$ the norms of the Lie products*

$$[x, \hat{a}] \qquad (x \in (E \dot{+} bE) \cap \Lambda)$$

over F form the set

$$\zeta^{\binom{n}{2}}\beta N(\hat{a} - \hat{a}\sigma)\{N(x) \mid x \in \mathfrak{A}\}$$

when $\mathfrak{A}$ is the $\Lambda \cap E$-ideal

$$\mathfrak{A} = \{y \mid y \in (((b^{-1}E + E) \cap b^{-1}\Lambda) + b^{-1}E) \cap E)\}.$$

Proof Note that the minimal equation for b over F is

$$b^n - \beta = 0$$

so that

$$N(b) = \zeta^{\binom{n}{2}}\beta.$$

The remainder follows from (8b)–(8d).

The striking relationship between any two quadratic subfields of the ring of 2×2 matrices over the field F established by O. Taussky's theorem stating that the determinant of the commutator of any pair of generators of the two subfields is equal to a negative norm into F from each of the two extensions is generalized by the theorem only to pairs of subfields of the ring of $n \times n$ matrices over the field F such that one of them is a radical extension generated by an element transforming the other extension according to an automorphism of order n.

In order to test the general relationship between the cyclic extension $F(a)$ and the norm of the commutator $[\hat{a}, \hat{b}]$ where

$$\hat{b} = \sum_{k=0}^{n-1} a_k b^{k-1},\ a_k = P_k(a),\ \hat{a} = P(a);\ P_k(t) \in F[t],\ P(t) \in F[t];\ 1 \leq k \leq n$$

we use the split model with $\beta_1 = \beta_2 = \cdots = \beta_n = \gamma$

$$a = \begin{bmatrix} \alpha\sigma & & & & \\ & \alpha\sigma^2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & \alpha\sigma^n \end{bmatrix}, \qquad b = \gamma \begin{bmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & & 1 \\ 1 & 0 & \cdots & & 0 \end{bmatrix}$$

where we assume γ to be a solution of the equation

$$\gamma^n = \beta \tag{14a}$$

It follows that

$$[\hat{a}, \hat{b}] = \sum_{i,k} ((P(\alpha\sigma^i) - P(\alpha\sigma^k))P_{(i-k)_n}(\alpha\sigma^i)\gamma^{(i-k)_n})$$

$$\left((-i-k)_n = \begin{cases} i-k & \text{if } i-k \geq 0 \\ i-k+n & \text{if } i-k < 0, \end{cases} \qquad 1 \leq i \leq n,\ 1 \leq k \leq n\right)$$

so that the norm of the commutator of $\hat{a}$, $\hat{b}$ appears as the determinant of the matrix on the right, which turns out to be a homogeneous form of degree n in both the coefficients of P as well as (jointly) in the coefficients of the P_k. In the cubic case there appears the simple result

$$N([\hat{a}, a_0 + ba_1 + b^2a_2]) = N(\hat{a}\sigma - \hat{a})(\beta N(a_1) - \beta^2 N(a_2))$$
$$(a_0, a_1, a_2 \in E,\ n = 3). \tag{14b}$$

In general there appears a norm form with many terms.

A deeper question concerns the Lie algebra characteristics of the direct decomposition (8a). This question will be discussed in Section 3.

3. The Spectral Decomposition Belonging to Maximal Commutative Subalgebras

It is well known that a ring H always is a bimodule relative to any subring E of H.

Let us follow up this remark by a more detailed analysis in case H is a unital hypercomplex system over a field F and E is a commutative F-subalgebra containing 1_H.

In that case we interpret H as a representation space of the tensor algebra $E^{(2)} = E \otimes_F E$, a unital commutative hypercomplex system over F, according to the operational rule

$$E^{(2)} \to \mathrm{End}_F\ H\colon \Delta$$

$$h((a_1 \otimes a_2)\Delta) = a_1 h a_2 \qquad (h \in H; \quad a_1, a_2 \in E). \tag{15a}$$

Let $e_1, e_2, \ldots, e_s$ be the primitive idempotents of E. It follows that the idempotents $e_i \times e_k$ of $E^{(2)}$ form a system of orthogonal idempotents of $E^{(2)}$ adding up to $1_{E^{(2)}} = 1 \times 1$. Accordingly, we obtain the decomposition

$$H = \sum_{i=1}^{s} \sum_{k=1}^{s} e_i H e_k \tag{15b}$$

of H into the direct sum of the E-bimodules $e_i H e_k$ which are characterized as the set of all elements of H with e_i as left identity and e_k as right identity.

The multiplicative interaction of the components is given by the rule

$$(e_i H e_k)(e_{i'} H e_{k'}) \subseteq \delta_{k,i'} e_i H e_{k'} \qquad (i, k, i', k' = 1, 2, \ldots, 1), \tag{15c}$$

which implies the Lie interaction rule

$$[e_i H e_k, e_{i'} H e_{k'}] \subseteq \delta_{k,i'} e_i H e_{k'} + \delta_{k',i} e_{i'} H e_k . \tag{15d}$$

We remark that the subalgebras $e_i H e_i$ of H are certainly simple F-subalgebras in the event that H is centrally simple over F.

In order to make further progress assume now that:

(1) H is centrally simple over F, of degree n;

(2) E is a subfield of H that is a maximal commutative subring, in other words E is an extension of $F1_H$;

(3) E is separable over F.

It follows that $E^{(2)}$ is semisimple. Hence there are finitely many primitive idempotents $d_1, \ldots, d_q$ of $E^{(2)}$ that are orthogonal adding up to 1. $E^{(2)}$ is the direct sum of the minimal ideals $E^{(2)}d_k$ $(1 \leq k \leq q)$. Correspondingly, we find the decomposition

$$H = \sum_{k=1}^{q} H d_k \tag{15e}$$

of H into the direct sum of the E-bimodules Hd_k which are characterized as the set of all elements of H with d_k as right identity. Let us number the d_k in such a way that the kernel of the diagonal F-epimorphism

$$E^{(2)} \to E: \delta$$

$$(a_1 \times a_2)\delta = a_1 a_2 \qquad (a_1, a_2 \in E) \tag{15f}$$

coincides with the maximal ideal

$$\sum_{k=2}^{q} E^{(2)} d_k .$$

It follows that δ restricts on $E^{(2)}d_1$ to an F-isomorphism onto the E-bimodule containing E.

As a matter of fact Hd_1 consists of all elements of H centralizing E so that by assumption

$$Hd_1 = E = E^{(2)}d_1\delta.$$

The E-bimodule H is operator isomorphic to the E-bimodule $E^{(2)}$. Indeed, there is a regular element x of H for which $x^{-1}Ex \cap E = F$. Hence

$$H = x^{-1}ExE = ExE$$

and the mapping

$$E^{(2)} \to H: \iota$$

$$(a_1 \underset{F}{\times} a_2)\iota = a_1 x a_2 \qquad (a_1, a_2 \in E)$$

provides an $E^{(2)}$-operator isomorphism.

In order to discuss the multiplicative interaction of the components let us begin with the case that E is a normal extension, which is tantamount to $q = n$ or, equally well, to the statement that each component Hd_k is n-dimensional over F. Denoting by G the automorphism group of E over F we may number the primitive idempotents of $E^{(2)}$ by the elements of G, say $d(\sigma)$ $(\sigma \in G)$ in such a way that

$$ad(\sigma) = d(\sigma)(a\sigma) \qquad (a \in E) \tag{15g}$$

$$Ed(\sigma) = d(\sigma)E = E^{(2)}d(\sigma) \tag{15h}$$

$$ad(\sigma)\iota = d(\sigma)\iota(a\sigma) \qquad (a \in E) \tag{15i}$$

$$Ed(\sigma)\iota = d(\sigma)\iota E = Hd(\sigma), \tag{15j}$$

and the elements y of the component $Hd(\sigma)$ of the direct decomposition (15c) are characterized by the relation

$$ay = y(a\delta) \qquad (a \in E). \tag{15k}$$

Since for σ, τ of G we have

$$ad(\sigma)\iota d(\tau)\iota = d(\sigma)\iota(a\sigma)d(\tau)\iota = d(\sigma)\iota d(\tau)\iota(a\sigma)\tau,$$

it follows that

$$d(\sigma)\iota d(\tau)\iota = d(\sigma\tau)\iota c(\sigma, \tau) \tag{15l}$$

where

$$c(\rho, \sigma)\tau c(\rho\sigma, \tau) = c(\rho, \sigma\tau)c(\sigma, \tau) \tag{15m}$$

$$d(1_G)\iota = 1_H, \qquad c(1_G, 1_G) = 1_E = 1_H \tag{15n}$$

$$Hd(\sigma)\sigma Hd(\tau) = Hd(\sigma\tau) \tag{15o}$$

$$[Hd(\sigma), Hd(\tau)] \subseteq Hd(\sigma\tau) + Hd(\tau\sigma) \tag{15p}$$

$$[y, a] = y(a - a\sigma) \qquad (y \in Hd(\sigma), \quad \sigma \in G, \quad a \in E). \tag{15q}$$

The last two results show that the decomposition

$$LH = \sum_{\sigma \in G}^{\cdot} Hd(\sigma) \tag{15r}$$

of the E-Lie algebra LH associated with H into the direct sum of linear subspaces over F is the spectral decomposition of LH with respect to the abelian subalgebra

$$LE = Hd(1_G) \tag{15s}$$

that is associated with E.

In the general case we embed E into a minimal splitting extension of E over F and we embed Φ as maximal abelian F-subalgebra into the ring of matrices H_1 of degree $[\Phi : E]$ over H. Hence $E = \Phi \cap H$.

Let G be the group of automorphisms of Φ over E, let $S = \mathrm{Aut}(\Phi/E)$ and let

$$\Phi^{(2)} = \Phi \underset{F}{\otimes} \Phi = \sum_{\sigma \in G}^{\cdot} \Phi^{(2)} d(\sigma)$$

where the $d(\sigma)$ are primitive idempotents of $\Phi^{(2)}$ such that

$$ad(\sigma) = d(\sigma)a\sigma \qquad (\sigma \in G, \quad a \in \Phi)$$

and ι is a $\Phi^{(2)}$-isomorphism of the regular Φ-bimodule $\Phi^{(2)}$ on H_1 mapping $\Phi^{(2)}d(1_G)$ on Φ. Hence there is the direct decomposition

$$H_1 = \sum_{\sigma \in G}^{\cdot} H_1 d(\sigma) \tag{16a}$$

of the Φ-bimodule H_1 with components

$$H_1 d(\sigma) = \{y(y \in H_1 \ \& \ \forall a(a \in \Phi \Rightarrow ay = y(a\sigma))\}. \tag{16b}$$

The tensor algebra

$$E^{(2)} = E \underset{F}{\otimes} E = \sum_{k=1}^{q}{}^{\cdot} E^{(2)} d_k \tag{16c}$$

with primitive idempotents $d_1, \ldots, d_q$ is a subalgebra of $\Phi^{(2)}$ such that $d_1 = d(1)$. The question is, which way is the direct decomposition of the E-bimodule $H = \sum_{k=1}^{q}{}^{\cdot} Hd_k$ related to the Remak decomposition (16a)?

Any idempotent of $\Phi^{(2)}$ is of the form

$$d(\mathfrak{R}) = \sum_{\sigma \in \mathfrak{R}} d(\sigma) \tag{16d}$$

where $\mathfrak{R}$ is a nonempty subset (complex) of G. The question is, which complexes are involved in the presentation of idempotents d_k?

Choose an F-basis $b_1, \ldots, b_n$ of E. Any element of $E^{(2)}$ is of the form $x = \sum_{i=1}^{n} b_i \times x_i$ with x_i uniquely determined by x in E and

$$x = x1 = x \sum_{\sigma \in G} d(\sigma) = \left(\sum_{i=1}^{n} b_i \times x_i \right) d(\sigma)$$

$$= \sum_{i=1}^{n} \sum_{\sigma \in G} b_i d(\sigma) x_i = \sum_{i=1}^{n} \sum_{k=1}^{q} \sum_{j=1}^{q_k} d(S\sigma_k\sigma_{kj})(b_i\sigma_k\sigma_{kj})x_i$$

where $G = \bigcup_{k=1}^{q} S\sigma_k S$, $S\sigma_k S = \bigcup_{j=1}^{q_k} S\sigma_k\sigma_{kj}$ with σ_{kj} in S and $\sum q_k = n$. If $x = d(\mathfrak{R})$, then

$$\sum_{i=1}^{n} (b_i\sigma_k\sigma_{kj})x_i = \begin{cases} 1 & \text{if } S\sigma_k\sigma_{kj} \subseteq \mathfrak{R} \\ 0 & \text{if } S\sigma_k S \not\subseteq \mathfrak{R}. \end{cases} \tag{16e}$$

On the other hand, the system of linear homogeneous equations

$$\sum_{i=1}^{n} (b_i\sigma_{k'}\sigma_{k'j'})x_i = y_{k'j'} \qquad (1 \le j \le q_k, \quad 1 \le k \le q)$$

$$(1 \le k' \le q_{k'}, \quad 1 \le k' \le q)$$

for the unknowns $x_1, \ldots, x_n$

has precisely one solution in Φ because of the separability of E over F. But upon application of an element σ of S to the system the n left-hand sides only are permuted though the x_i are changed to $x_i\sigma$. Hence, if $x_i \in E$, then the permutations connected with the elements σ of S leave the right-hand sides invariant.

This means that $\mathfrak{R}$ is a union of several double cosets $S\sigma_k S$. On the other hand, setting $y_{k'j'} = \delta_{kk'}$ we find that $x_i\sigma = x_i$ for all σ of S so that x_i belongs to E and $d(S\sigma_k S)$ belongs to $E^{(2)}$.

It follows that the primitive idempotents of $E^{(2)}$ are precisely the idempotents $d(S\sigma_k S)$ corresponding to the double cosets. Hence we have

$$d_k = d(S\sigma_k S) \tag{17}$$

after suitable numbering of $d_1, \ldots, d_q$. Thus the multiplication rules

$$Hd_kHd_{k'} = Hd(S\sigma_k S\sigma_{k'} S) \tag{18a}$$

and the Lie multiplication rules

$$[Hd_k, Hd_{k'}] \subseteq Hd(S\sigma_k S\sigma_{k'} S) + Hd(S\sigma_{k'} S\sigma_k S)$$
$$(1 \leq k \leq q, \quad 1 \leq k' \leq q) \tag{18b}$$

emerge. It should be noted that for any set of double cosets

$$\{S\sigma_{k_1} S, \ldots, S\sigma_{k_m} S \,|\, 1 \leq k_1 < k_2 < \cdots < k_m \leq q\}$$

we have the rules

$$d\left(\dot{\bigcup_{i=1}^{m}} S\sigma_{k_i} S\right) = \sum_{i=1}^{m} d(S\sigma_{k_i} S) \tag{19}$$

$$Hd\left(\dot{\bigcup_{i=1}^{m}} S\sigma_{k_i} S\right) = \sum_{i=1}^{m} Hd_{k_i} \tag{20}$$

which tell us all worthwhile knowing about the evaluation of the right-hand side of (18a), (18b).

4. Crossed Product Rings

For any unital ring R there is the canonical homorphism

$$U(R) \to \mathrm{Aut}(R): \theta$$
$$a(x\theta) = x^{-1}ax \qquad (a \in R, \quad x \in U(R)) \tag{21}$$

of the unit group $U(R)$ of R into the automorphism group, $\mathrm{Aut}(R)$, of R. Its image is a normal subgroup $\mathrm{Inn}(R)$ of $\mathrm{Aut}(R)$, the *inner automorphism group of* R, which is normal in $\mathrm{Aut}(R)$ according to the transformation rule

$$\alpha^{-1}(x\theta)\alpha = (x\alpha)\theta \qquad (x \in U(R), \quad \alpha \in \mathrm{Aut}(R)). \tag{22}$$

The factor group is the *outer automorphism group of* R

$$\mathrm{Out}(R) = \mathrm{Aut}(R)/\mathrm{Inn}(R).$$

Supposing R is contained in a unital overring Λ such that

$$1_\Lambda = 1_R. \tag{23a}$$

The normalizer of R relative to the unit group $U(\Lambda)$ of Λ is defined as the subgroup

$$N_{U(\Lambda)}(R) = \{x \,|\, x \in U(\Lambda) \,\&\, x^{-1}Rx = R\} \tag{23b}$$

of $U(\Lambda)$ containing $U(R)$ as normal subgroup.

For any subgroup H of $N_{U(\Lambda)}(R)$ we have the relations

$$hR = Rh \qquad (h \in H) \tag{23c}$$

so that R and H generate the subring

$$HR = \langle R, H \rangle = RH \tag{23d}$$

of Λ. We set ourselves the task of studying the structure of HR in terms of H and R.

Analysis of the Problem

Without loss of generality it may be assumed that

$$U(R) \subseteq H \subseteq N_{U(\Lambda)}(R), \tag{24a}$$

$$HR = \Lambda = RH. \tag{24b}$$

We observe that the kernel of the homomorphism

$$\begin{aligned} &H \to \mathrm{Aut}(R): \varphi \\ &a(h\varphi) = h^{-1}ah \qquad (a \in R, \quad h \in H) \end{aligned} \tag{24c}$$

is the centralizer of R in $U(\Lambda)$:

$$C_{U(\Lambda)}(R) = \{x \mid x \in U(\Lambda) \,\&\, \forall a(a \in R \Rightarrow xa = ax)\}$$

and that the kernel of the corresponding homomorphism of H into the outer automorphism group of R

$$\begin{aligned} &H \to \mathrm{Out}(R): \bar{\varphi} \\ &h\bar{\varphi} = h\varphi/\mathrm{Inn}(R) \qquad (h \in H) \end{aligned} \tag{24d}$$

is the product of the two normal subgroups $U(R)$, $(C_{U(\Lambda)}(R)) \cap H$. The ring $R_1 = \langle R, C_{U(\Lambda)}(R) \rangle$ generated by R and $C_{U(\Lambda)}(R)$ is the product of the two elementwise commuting subrings R and $R_0 = \langle C_{U(\Lambda)}(R) \rangle$ intersecting in a subring of the center ${}_3R$ of R. There hold the relations

$$hR_1 = R_1 h$$

for any element h of H so that

$$\langle R, H \rangle = HR_1 = R_1 H = \sum_{h \in H} hR_1.$$

Without loss of generality we can also assume that

$$C_{U(\Lambda)}(R) \subseteq {}_3R, \qquad \ker \bar{\varphi} = U(R). \tag{24e}$$

Hence we have the exact sequences

$$\begin{aligned} &1 \to U(R) \xrightarrow{i_1} H \xrightarrow{\varepsilon_1} S \to 1, \\ &1 \to U({}_3R) \xrightarrow{U({}_3R)|i_1} H \xrightarrow{\varphi} \mathrm{Aut}(R) \end{aligned} \tag{24f}$$

and the conditions

$$R^H = \{a | a \in R \,\&\, \forall h | h \in H \Rightarrow a = a(h\varphi)\} \subseteq {}_3(R), \qquad \iota_1\varphi = \theta \quad (24g)$$

when ι_1 is the natural embedding monomorphism of $U(R)$ in H, ε_1 is the natural epimorphism of H on the factor group $S = H/U(R)$, and φ is a monomorphism of H in $\mathrm{Aut}(R)$.

Thus H emerges as a special kind of group theoretic extension of the unit group of $U(R)$ characterized by (21), (24a)–(24c), (24e), and (24f) which we will call an *R-admissable extension* of $U(R)$.

Our task is to describe the rings Λ satisfying (24a) and (24b) in terms of the R-admissable extension H of $U(R)$.

Definition The *crossed product* of a unital ring R and R-admissable extension H of the unit group $U(R)$ of R is defined as the ring $R \times H$ with the generators $\bar{a}(a \in R)$, $\bar{h}(h \in H)$ and the defining relators

$$\bar{a}_1 + \bar{a}_2 = \overline{a_1 + a_2}, \quad \bar{a}_1\bar{a}_2 = \overline{a_1 a_2} \qquad (a_1, a_2 \in R), \quad (25a)$$

$$\bar{h}_1\bar{h}_2 = \overline{h_1 h_2} \qquad (h_1, h_2 \in H), \quad (25b)$$

$$\overline{x\iota_1} = \bar{x} \qquad (x \in U(R)), \quad (25c)$$

$$\bar{h}^{-1}\bar{a}\bar{h} = \overline{a(h\varphi)} \qquad (a \in R, \quad h \in H). \quad (25d)$$

Theorem 2 (a) *The mapping*

$$R \to R \times H: \iota_2$$
$$a\iota_2 = \bar{a} \qquad (a \in R) \quad (25e)$$

is a monomorphism of the ring R into the crossed product of R and H mapping the unit element of R on the unit element of $R \times H$.

(b) *The mapping*

$$H \to U(R \times H): \iota_3$$
$$h\iota_3 = \bar{h} \qquad (h \in H) \quad (25f)$$

is a monomorphism of H into the unit group of the crossed product of R and H such that

$$\iota_1\iota_3 = U(R)|\iota_2 \quad (25g)$$

and

$$H\iota_3 R\iota_2 = R \times H = R\iota_2 H\iota_3, \quad (25h)$$

$$N_{U(R\times H)}(R\iota_2)R\iota_2 = R \times H = R\iota_2 N_{U(R\times H)}(R\iota_2), \quad (25i)$$

$$C_{U(R\times H)}(R\iota_2) = {}_3R\iota_2. \quad (25j)$$

(c) *Identifying R with $R\iota_2$ via the embedding monomorphism ι_2 and H with $H\iota_3$ via the embedding monomorphism ι_3 the crossed product of R and H appears as the universal solution of our task of which all other solutions are obtained by the application of an R-epimorphism.*

Proof Let T a transversal of H modulo $U(R)\iota$, such that

$$H = T(U(R)\iota_1) = (U(R)\iota_1)T,$$

$$T \cap T(x\iota_1) \quad \text{is empty whenever} \quad 1 \neq x \in U(R),$$

$$1_H \in T, \tag{26a}$$

$$t't'' = t(c(t', t'')\iota_1) \qquad (t', t'', t \in T; \quad c(t', t'') \in U(R)). \tag{26b}$$

The set $(R \times H)^*$ of all formal sums $\sum_{t \in T} t(ta)$ (a any mapping of T in R with only a finite number of elements of T with nonzero image) with the operational rules

$$\sum_{t \in T} t(ta) = \sum_{t \in T} t(tb) \Leftrightarrow a = b, \tag{26c}$$

$$\sum_{t \in T} t(ta) + \sum_{t \in T} t(tb) = \sum_{t \in T} t(t(a + b)), \tag{26d}$$

$$\left(\sum_{t \in T} t(ta)\right) \sum_{t \in T} t(tb) = \sum_{t \in T} t(t(a \times b)), \tag{26e}$$

where the mapping $a \times b$ of T in R is defined by setting

$$t(a \times b) = \sum_{\substack{t' \in T,\, t'' \in T \\ t't''U(R) = tU(R)}} c(t', t'')((t'a(t''\varphi))(t''b)),$$

is verified to be a ring by an easy computation. The mapping of $\bar{a}$ on $1_H a$ ($a \in U(R)$) and of $t(x\iota_1)$ on tx ($t \in T$, $x \in U(R)$) preserves the defining relators of $R \times H$ as another easy computation shows. Moreover, the elements $1_H a$, tx of above generate $(R \times H)^*$. Hence the mapping of above extends uniquely to an epimorphism ε of $R \times H$ on $(R \times H)^*$.

On the other hand for any solution Λ of our task the mapping of the formal sum $\sum_{t \in T} t(ta)$ on the corresponding sums defined in Λ preserves the operational rules (26d) and (26e) as a third computation will show. Thus it is shown that ε is an isomorphism and that (26c) holds.

The mapping of a on $1_H a$ ($a \in R$) turns out to be a monomorphism of R in $(R \times H)^*$. Thus (a) is demonstrated. Note that $1_H a$ is the unit element of $(R \times H)^*$. The mapping of $t(x\iota_1)$ on tx ($t \in T$, $x \in U(R)$) turns out to be a monomorphism of H into $N_{U((R \times H)^*)}(1_H R)$ mapping $x\iota_1$ on $1_H x$ ($x \in U(R)$). Thus (25b), (25h), and (25i) are demonstrated.

Finally let us consider those elements $z = 1_H a$ ($a \in R$) which commute with all elements tx ($t \in T$, $x \in U(R)$). Each element h of H is of the form $h = t(x\iota_2)$ for some t of T, x of $U(R)$ and conversely; the commutativity

relation $z(tx) = (tx)z$ is tantamount to $z(h\varphi) = z$. Hence according to (24f) we have $z \in \mathfrak{z}(R)$, demonstrating the remainder of Theorem 2.

Extension Invariance

One of the criteria applied to any algebraic construction is the question how well it behaves in regard to an extension of the basic domain of rationality.

Suppose the given unital ring R is embedded by means of an embedding monomorphism

$$R \to \Omega\colon \iota_R \tag{27a}$$

into a unital ring Ω such that the unit element of R is mapped by ι_R on the unit element of Ω.

Is it possible to embed a crossed product of R with an R-admissible extension H of $U(R)$ into a crossed product of Ω with some Ω-admissible extension H_Ω of $U(\Omega)$ such that the embedding monomorphism

$$R \times H \to \Omega \times H_\Omega\colon \iota_{R\times H} \tag{27b}$$

restricts to ι_R on R but to a monomorphism into H_Ω on H and that the ring $\Omega \times H_\Omega$ is the ring generated by the subrings $(R \times H)\iota_{R\times H}$, Ω? Is it true that $H_\Omega = H_{\iota_{R\times H}} U(\Omega)$?

We observe that necessarily the homomorphism

$$H_\Omega \to \mathrm{Aut}(\Omega)\colon \varphi_\Omega \tag{27c}$$

inherent in the construction of $\Omega \times H_\Omega$ restricts to a homomorphism $H_{\iota_{R\times H}}|\varphi_\Omega$ for which

$$(a\iota_R)(h\varphi_\Omega) = \alpha(h\varphi) \qquad (a \in R, h \in H), \tag{27d}$$

a condition which restricts our choice of Ω.

We consider only the case that Ω is the tensor product of the ring R and a unital overring S of the central subring R^H of R over R^H:

$$\Omega = R \underset{R^H}{\otimes} S \tag{27e}$$

when it is required that

$$1_S = 1_{R^H}$$

and that the canonical embedding homomorphism (27a) mapping a on $a \otimes 1_S$ $(a \in R)$ is a monomorphism. Without loss of generality the canonical homomorphism

$$S \to \Omega\colon \iota_S$$

$$s\iota_S = 1_R \otimes s \qquad (s \in S)$$

can be assumed to be monomorphic.

Now there is the canonical homomorphism (27c) given by setting

$$(a \otimes s)(h\varphi_\Omega) = (a(h\varphi)) \times s \tag{27f}$$

satisfying (27d).

The condition (27b) requires H_Ω to be a homomorphic image of the amalgamated semidirect product of H and the unit group of Ω over $U(R)$, say

$$H \underset{\varphi\Omega}{\overset{U(R)}{\square}} U(\Omega).$$

Here quite generally we define the amalgamated semidirect product

$$A \underset{\Psi}{\overset{N}{\square}} B$$

of two groups A, B over a common normal subgroup N as follows.

We assume N to be a normal subgroup of A with given monomorphism ι_N into B such that $N\iota_N$ is a normal subgroup of B. Furthermore there is a homomorphism Ψ of A into the automorphism group of B given satisfying the coherence condition

$$n\theta_A \Psi = n\iota_B \theta_B \qquad (n \in N) \tag{27g}$$

when θ_A, θ_B denote the canonial epimorphism of the elements of A, B, respectively, on the corresponding inner automorphism groups. Let

$$A \underset{\Psi}{\overset{N}{\square}} B = \{a \square b \,|\, a \in A, \quad b \in B\} \tag{27h}$$

with multiplication rule

$$(a \square b)(a' \square b') = (aa') \square (b(a\Psi)b') \tag{27i}$$

and equality rule

$$(a, a' \in A; b, b' \in B) \quad a \square b = a' \square b' \Leftrightarrow a'^{-1}a \in N \;\&\; a'^{-1}a\iota_N = b'b^{-1}.$$

One verifies easily that $A \square_\Psi^N B$ is a group with canonical embedding monomorphisms

$$A \to A \underset{\Psi}{\overset{N}{\square}} B\colon \iota_A, \quad B \to A \underset{\Psi}{\overset{N}{\square}} B\colon \iota_B$$

$$a\iota_A = a \square 1_B, \quad b\iota_B = 1_A \square b$$

satisfying the coherence condition

$$N\,|\,\iota_A = \iota_N \iota_B, \tag{27k}$$

moreover

$$N\iota_A \lhd A \underset{\Psi}{\overset{N}{\square}} B, \quad B\iota_B \lhd A \square B, \tag{27l}$$

$$(A\iota_A)(B\iota_B) = A \underset{\Psi}{\overset{N}{\square}} B, \quad A\iota_A \cap B\iota_B = N\iota_A. \tag{27m}$$

A particular example are the semidirect products of A, B arising whenever $N = 1$. We denote them simply as $A \square_\Psi B$.

Continuing with the construction of an extension of the given crossed product $R \times H$ by means of the tensor product (27e) we let

$$H_\Omega = H \underset{\varphi\Omega}{\overset{U(R)}{\square}} U(\Omega), \tag{27n}$$

$$H_\Omega \to \mathrm{Aut}(\Omega)\colon \varphi_\Omega^*$$

$$(h \square \varepsilon)\varphi_\Omega^* = h\varphi_\Omega(\varepsilon\theta_\Omega) \tag{27o}$$

($h \in H$, $\varepsilon \in U(\Omega)$, θ_Ω the canonical epimorphism of $U(\Omega)$ on $\mathrm{Inn}(\Omega)$). It follows that H_Ω is an Ω-admissible extension of $U(\Omega)$ such that the crossed product $\Omega \times H_\Omega$ is an extension of $R \times H$ in the sense defined in the beginning of this section. Let us observe the isomorphy relation

$$\Omega \times H_\Omega \simeq (R \times H) \underset{R^H}{\otimes} S \tag{27p}$$

with canonical isomorphism mapping the element $(a \otimes s)(h \square \varepsilon)$ on $(ah \otimes s)\,\varepsilon$ ($a \in R$, $s \in S$, $h \in H$, $\varepsilon \in U(\Omega)$).

Examples

(a) The group ring $R[G]$ of a group G over a unital ring R is a crossed product of the subring $R[N]$ and G for any normal subgroup N of G that contains its centralizer in G according to

$$R[G] = R[N] \times GU(R[N]). \tag{28a}$$

(b) Suppose R is a unital ring with primitive idempotents $E_1, \ldots, E_\sigma$ of the center of R such that $E_1 + \cdots + E_\sigma = 1_R$ and H is an R-admissible extension of $U(R)$, then the automorphism group $H\varphi$ permutes the finite set $S = \{E_1, \ldots, E_\sigma\}$ such that S is partitioned into a finite number $S_1, \ldots, S_\sigma$ of $H\varphi$-orbits. It follows that the idempotents

$$E_{S_j} = \sum_{E_i \in S_j} E_i \qquad (1 \leq j \leq \sigma)$$

are invariant under the automorphisms of R belonging to $H\varphi$ and that

the idempotents $E_{S_1}, \ldots, E_{S_\sigma}$ are orthogonal idempotents of the center of the crossed product $R \times H$ with the unit element as their sums so that there is the split

$$R \times H = \sum_{j=1}^{\sigma} \cdot E_{S_j}(R \times H)$$

of $R \times H$ into the direct sums of σ ideals of $R \times H$.

For each of those ideals let us form the centralizer $C_H(E_{S_j}R)$ of the subring $E_{S_j}R$ of $E_{S_j}(R \times H)$ relative to H and a transversal T_j of $C_H(E_{S_j}R)$ modulo the normal subgroup $C_H(E_{S_j}R) \cap U(R)$. It follows that the ring $E_{S_j}(R \times H)$ contains the subring

$$R_j = \sum_{t \in Tj} \cdot tE_{S_j}R$$

invariant under $H\varphi$ and that $E_{S_j}(R \times H)$ is a crossed product of R_j and $E_{S_j}H$ so that

$$R \times H \simeq \oplus_{j=1}^{\sigma} R_j \times E_{S_j}H. \tag{28b}$$

In this way the study of the crossed products for a ring R that is isomorphic to the algebraic sum of a finite number of algebraically indecomposable rings is reduced to the case that those indecomposable components are transitively permuted by the group of automorphisms $H\varphi$.

(c) Let us study the crossed product of a *semisimple ring* R with an R-admissible extension H of $U(R)$ such that the primitive idempotents $E_1, \ldots, E_\sigma$ of the center of R are transitively permuted by the automorphism group $H\varphi$. According to the second structure theorem of McLagan–Wedderburn there is the decomposition

$$R = \sum_{j=1}^{\sigma} \cdot R_j \qquad \text{when} \quad R_j = E_j R, \tag{29a}$$

of R into the discret sum of σ simple ideals. By construction the simple components of R are isomorphic to one another.

Let us analyze this situation!

For any simple ring R_1 there is the restriction homomorphism

$$\begin{aligned} &\text{Aut } R_1 \to \text{Aut}(\mathfrak{z}R_1): \mu_1 \\ &\quad \alpha\mu_1 = \mathfrak{z}R_1|\alpha \qquad (\alpha \in \text{Aut}(R_1)) \end{aligned}$$

of the automorphism group of R_1 into the automorphism group of $\mathfrak{z}R_1$.

Each automorphism α of R permutes the primitive idempotents of the center of R so that there is the permutation representation

$$\begin{aligned} &\text{Aut } R \to \mathfrak{p}_\sigma: \Delta \\ &\quad E_{j\alpha\Delta} = E_j\alpha \qquad (\alpha \in \text{Aut } R). \end{aligned} \tag{29b}$$

In fact

$$(\text{Aut } R)\Delta = \mathfrak{p}_\sigma \tag{29c}$$

and Aut R is the semidirect product of the kernel of Δ and the subgroup $\mathfrak{p}_\sigma$ formed by the automorphism

$$R \to R: \bar{\pi}$$

$$\left(\sum_{i=1} a_i \theta_i\right)\bar{\pi} = \sum_{i=1} a_i \theta_{i\pi} \tag{29d}$$

($\pi \in \mathfrak{p}_\sigma$, $a_i \in R_1$, θ_i an isomorphism of R_1 on R_i $(1 \leq i \leq \sigma)$, $\theta_1 = 1_{R_1}$).

The kernel of Δ consists of the automorphisms of R that leave every minimal ideal invariant. It is the direct product of the subgroups $\overline{\text{Aut}(R_i)}$ formed by the automorphisms of R fixing the complementary ideal of R_i in R element wise $(1 \leq i \leq \sigma)$.

There is the canonical monomorphism

$$\text{Aut } R_i \to \ker \Delta: v_i$$

$$\left(\sum_{j=1}^{\sigma} a_j \theta_j\right)\alpha v_i = a_i \theta_i \alpha + \sum_{\substack{j=1 \\ j \neq i}}^{\sigma} a_j \theta_j$$

$$(a_j \in R_1 (1 \leq j \leq \sigma), \quad \alpha \in \text{Aut } R_i) \tag{29e}$$

sending Aut R_i on $\overline{\text{Aut } R_i}$ and, of course, there are the isomorphisms

$$\text{Aut } R_i = \theta_i^{-1}(\text{Aut } R_1)\theta_i \tag{29f}$$

of Aut R_i and Aut R_1 for $i = 1, 2, \ldots, \sigma$.

In this way the automorphism group of R is seen to be isomorphic to the wreath product of $\mathfrak{p}_\sigma$ over the automorphism group of R_1, the outer automorphism group of R is isomorphic to the wreath product of $\mathfrak{p}_\sigma$ over the subgroup $\text{Aut}(R_1)\mu_1$ of $\text{Aut}(_3R_1)$:

$$\text{Aut } R \simeq \text{Aut } R_1 \wr \mathfrak{p}_\sigma, \tag{29g}$$

$$\text{Out } R \simeq \text{Out } R_1 \wr \mathfrak{p}_\sigma, \tag{29h}$$

$$\text{Aut } R_j \simeq \text{Aut } R_1 \qquad (1 \leq j \leq \sigma), \tag{29i}$$

$$\text{Out } R \simeq (\text{Aut } R_1)\mu_1. \tag{29j}$$

The factor group of an R-admissible extension H of $U(R)$ over $U(R)$ is isomorphic to a subgroup S of Aut R, in fact there is the exact sequence

$$1 \to U(R) \xrightarrow{i_1} H \xrightarrow{\varphi} S \to 1. \tag{29k}$$

By assumption the permutation group $H\Delta$ of σ letters is transitive.

Conversely, if S is a subgroup of $S\Delta$ such that $H_0 \mu\Delta$ is transitive and if there is the exact sequence (29k) for H find the crossed product $R \times H$ with the property that 1_R is the only idempotent of R invariant under $H\varphi$.

When is the crossed product simple? In view of the conjugacy of the orthogonal idempotents E_j $(1 \leq j \leq \sigma)$ under H the simplicity of $R \times H$ implies that the subalgebra $E_1(R \times H)E_1$ is simple.

If the element h of H does not belong to the H-centralizer H_1 of E_1, then there holds an equation

$$E_1 h = h\, E_j$$

with $j > 1$ so that $E_1 h E_1 = 0$. Hence

$$E_1(R \times H)E_1 = H_1 R_1 = R_1 H_1. \tag{30}$$

Furthermore the elements of H_1 commuting elementwise with R_1 form a normal subgroup H_1^* of H_1 such that

$$E_1 H_1^*\, E_1 \simeq H_1/\overline{\mathrm{Aut}\, R_1},$$
$$U(\mathfrak{z}R_1)\, \Delta\, E_1 H_1^* E_1,$$

there is a transversal T_1 of $E_1 H_1^* E_1$ over $U(\mathfrak{z}R_1)$ such that

$$E_1 H_1^* E_1 = T_1 U(\mathfrak{z}R_1), \quad T_1 \cap U(\mathfrak{z}R_1) = E_1,$$
$$xT_1 \cap U(\mathfrak{z}R_1) = \Phi \qquad (1 \neq x \in U(\mathfrak{z}R_1)),$$
$$U(\mathfrak{z}R_1)H_1^* = U(\mathfrak{z}R_1)T_1,$$

T_1 is linearly independent over $\mathfrak{z}R_1$ and $U(\mathfrak{z}R_1)T_1$ is the centralizer of R_1 in $R_1 H_1$.

The simplicity of $R_1 H_1$ implies simplicity of the centralizer of the simple subalgebra R_1. As can easily be shown, T_1 is finite. As the example provided by any quaternion algebra over a field of characteristic $\neq 2$ shows it can happen that T_1 consists of more than one element.

Conversely, if $C_{R_1 H_1} R_1$ is simple, then it follows from E. Artin's argument on nonvanishing sums of the form

$$\sum_{h \in X_1} h(ha)$$

(X_1 a transversal of H_1 modulo the normal subgroup N_1 of all elements n of H_1 for which $n\varphi$ belongs to $\mathrm{Inn}(R)$; a is a mapping of X_1 in R_1 with all but a finite number of images equal to zero) which are contained in a given ideal of $E_1(R \times H)E_1$ that the subring $E_1(R \times H)E_1$ is simple.

Now it follows from E. Artin's argument applied once again in another context that $R \times H$ is simple.

Theorem 3 (a) *Any semisimple ring R is of the form*

$$R = \sum_{j=1}^{\sigma} \cdot E_j R$$

where $E_1, \ldots, E_\sigma$ are the primitive idempotent elements of the center of R and the numbering is chosen in such a way that there are isomorphisms

$$E_{\sigma_k} R \to E_j R: \theta_j$$

$$(\sigma_{k-1} < j \leq \sigma_k, \quad \theta_{\sigma_k} = 1_{E_{\sigma k}} R, \quad 1 \leq k \leq \tau, \quad \tau > 0,$$

$$0 = \sigma_0 < \sigma_1 < \sigma_2 < \cdots < \sigma_\tau = \sigma)$$

but that the simple algebras $E_{\sigma_k} R$ are nonisomorphic for $k = 1, 2, \ldots, \tau$.

(b) *There is the permutation representation*

$$\mathrm{Aut}(R) \to \mathfrak{p}_\sigma: \Delta$$

$$E_j \alpha = E_{j\alpha\Delta} \qquad (\alpha \in \mathrm{Aut}(R), \quad 1 \leq j \leq \sigma)$$

with τ orbits $S_k = \{\sigma_{k-1} + 1, \ldots, \sigma_k\}$ $(1 \leq k \leq \tau)$.

(c) *The automorphism group of R is the direct product of the subgroups $(\mathrm{Aut}\ R)_k$ formed by the automorphisms of R which leave the idempotent*

$$E_{S_k} = \sum_{j=\sigma_{k-1}+1}^{\sigma_k} E_j$$

as well as every element of the complementary ideal $(1_k - E_{S_k})R$ of $E_{S_k} R$ fixed $(1 \leq k \leq \tau)$.

(d) *The direct component $(\mathrm{Aut}\ R)_k$ is isomorphic to the wreath product of $\mathrm{Aut}(R_{\sigma_k})$ and $\mathfrak{p}_{(\sigma_k - \sigma_{k-1})}$ $(1 \leq k \leq \tau)$.*

The outer automorphism group of $E_{S_k} R$ is isomorphic to the wreath product of $(\mathfrak{z}R_{\sigma_k})|\mathrm{Aut}(R_{\sigma_k})$ and $\mathfrak{p}_{(\sigma_k - \sigma_{k-1})}$ $(1 \leq k \leq \tau)$.

(e) *The crossed product of R and an R-admissible extension H of $U(R)$ is simple precisely, if $\tau = 1$, $H\varphi\Delta$ is transitive and the centralizer of the projective group algebra $\mathfrak{z}(E_1 R) \otimes_{U(\mathfrak{z}(E_1 R))} C_H E_1 R$ is simple.*

It is a hypercomplex system over some field precisely if (e) *is satisfied and if $\mathfrak{z}(R)$ is of finite dimension over the field $C_R(H)$, i.e., $C_H(E_1 R)$ is of finite index in $C_H(E_1)$.*

It is of the O. Teichmüller type precisely if (in addition) R is commutative and $C_H(E_1) = C_H(E_1 R)$.

It is of the classical A. Albert–R. Brauer–H. Hasse–E. Noether type if (in addition) R is a field.

It is of the Dickson–Wedderburn type if (in addition) R is a finite cyclic extension of R^H.

Corollary *The automorphism group of a ring of matrices* $R = R_0^{f \times f}$ *over the unital commutative ring* R_0 *is the semidirect product of the centralizer of the matrix units in* Aut(R) *and the inner automorphism group. The first factor is isomorphic to the automorphism group of* R_0 *with the canonical isomorphism which maps the matrix* (a_{ik}) *on the matrix* $(a_{ik}\alpha)$ *for* α *in* $\mathrm{Aut}(R_0)$.

5. Crossed Product Orders

Let E be a semisimple ring and let H be an E-admissible extension of $U(E)$ such that the crossed product $A = E \times H$ is simple of finite dimension over the center $F = E^H$.

In this section we study the arithmetics of certain orders of A over dedekind rings R of F with F as quotient field which are related to the presentation of A as a crossed product.

Definition The R-order Λ of A is said to be a *crossed product order* relative to the given presentation of A as crossed product over E if there holds the decomposition

$$\Lambda = \sum_{i=1}^{H:U(F)} {}^{\cdot} \Lambda \cap (H_i E) \tag{31a}$$

of Λ into the direct sum of the intersections of Λ with the crossed product components of A, where

$$H = \bigcup_{i=1}^{H:U(F)} {}^{\cdot} H_i, \qquad H_1 = U(E) \tag{31b}$$

is the coset decomposition of H modulo $U(E)$ and where

$$A = \sum_{i=1}^{H:U(F)} {}^{\cdot} H_i E, \tag{31c}$$

$$(\Lambda \cap H_i E)(\Lambda \cap H_j F) = \Lambda \cap H_i H_j E \qquad (i, j = 1, 2, \ldots, H : U(E)). \tag{31d}$$

We observe that because of (31a) a crossed product order Λ satisfies the invariance condition

$$N_H(\Lambda \cap U(E))U(E) = H. \tag{31e}$$

Theorem 4 (Benz–Zassenhaus) *Let A be absolutely semisimple over F. Every crossed product order* Λ *is embedded into a crossed product order* Λ^{**} *intersecting with E in a hereditary order such that the embedding is invariant under all F-automorphisms of A.*

The intersection of all maximal orders of A containing Λ^{**} is a hereditary order Λ^* of A.

Proof "Hereditary orders" emerged in the theory of orders as an appropriate generalization of "maximal orders" first conceived by Auslander and Goldman and independently by H. Benz about twenty years ago. Of the many equivalent definitions of hereditary orders of a semisimple hypercomplex system B over F let us mention the following definitions.

(H1) The order of B is said to be hereditary if any Λ-sublattice M_1 of a Λ-lattice M has a complement in M precisely if the Λ-factor module M/M_1 is a Λ-lattice (Auslander–Goldman).

(H2) The order Λ of B is hereditary precisely if for every prime ideal $\mathfrak{P}$ of R the $\mathfrak{P}$-radical of Λ, i.e., the ideal $J_{\mathfrak{P}}(\Lambda)$ of Λ containing $\mathfrak{P}\Lambda$ with the property that $J_{\mathfrak{P}}(\Lambda)/\mathfrak{P}\Lambda$ is the maximal nilpotent ideal of $\Lambda/\mathfrak{P}\Lambda$, is invertible relative to Λ (Auslander–Goldman).

(H3) The order Λ of B is hereditary precisely if for any prime ideal $\mathfrak{P}$ of Λ the left order of $J_{\mathfrak{P}}(\Lambda)$, i.e., the R-dedekind module

$$[J_{\mathfrak{P}}(\Lambda)/J_{\mathfrak{P}}(\Lambda)] = \{a \,|\, a \in A \in aJ_{\mathfrak{P}}(\Lambda) \subseteq J_{\mathfrak{P}}(\Lambda)\},$$

coincides with Λ (Zassenhaus).

(H4) The order Λ of B is hereditary precisely if for any prime ideal $\mathfrak{P}$ of Λ the right order of $J_{\mathfrak{P}}(\Lambda)$, i.e., the R-dedekind module

$$[J_{\mathfrak{P}}(\Lambda)\backslash J_{\mathfrak{P}}(\Lambda)] = \{b \,|\, b \in A \in J_{\mathfrak{P}}(\Lambda)b \subseteq J_{\mathfrak{P}}(\Lambda)\}$$

coincides with Λ (Zassenhaus).

(H5) The order Λ of B is hereditary precisely if for any prime ideal $\mathfrak{P}$ of Λ its A-idealizer, i.e., the R-dedekind module

$$[J_{\mathfrak{P}}(\Lambda)/J_{\mathfrak{P}}(\Lambda)] \cap [J_{\mathfrak{P}}(\Lambda)\backslash J_{\mathfrak{P}}(\Lambda)],$$

coincides with Λ (Zassenhaus).

(H6) The order Λ of B is hereditary precisely if for any prime ideal $\mathfrak{P}$ of R the $\mathfrak{P}$-localization of Λ, i.e., the $(R/(R - \mathfrak{P}))$-order

$$\frac{\Lambda}{R - \mathfrak{P}} = \{\lambda^{-1}a \,|\, a \in \Lambda \;\&\; \lambda \in R, \lambda \notin \mathfrak{P}\}$$

is hereditary over the $\mathfrak{P}$-localization

$$\frac{R}{R - \mathfrak{P}} = \{\lambda^{-1}r \,|\, r \in R \;\&\; \lambda \in R, \lambda \notin \mathfrak{P}\},$$

of R (Auslander–Goldman).

(H7) The order Λ of B is hereditary precisely if for any prime ideal $\mathfrak{P}$ of R the $\mathfrak{P}$-adic completion of Λ, i.e., the $R_{\mathfrak{P}}$-order $\Lambda_{\mathfrak{P}}$ of all $\mathfrak{P}$-adic limits of

$\mathfrak{P}$-adic convergent sequences of elements of Λ, is a hereditary order over the $\mathfrak{P}$-adic completion ring $R_{\mathfrak{P}}$ of R (Auslander–Goldman).

(H8) The order Λ of B over R is hereditary precisely if the intersections of Λ with the simple components of B are hereditary over R and if Λ is the direct sum of its intersections with the simple components of B (Auslander–Goldman).

(H9) The order Λ of a commutative semisimple hypercomplex system B over the quotient field F of a dedekind ring R is hereditary precisely if it is the maximal order $\Lambda(B, R)$ of B over R (Auslander–Goldman).

(H10) The order Λ of a division ring B of finite dimension over the quotient field F of a complete local dedekind ring R is hereditary precisely if it is the maximal order $\Lambda(B, R)$ of B over R (Auslander–Goldman).

(H11) The order Λ of B isomorphic to the ring of matrices $D^{f\times f}$ of a division ring D of finite dimension over the quotient field F of a complete local dedekind ring R is hereditary precisely if D and the f^2 matrix units e_{ik} $(i, k = 1, 2, \ldots, f)$ for which

$$e_{\alpha\beta}e_{\alpha'\beta'} = \delta_{\beta\alpha'}e_{\alpha\beta'}, \qquad e_{\alpha\beta}\lambda = \lambda e_{\alpha\beta}$$

$$(\alpha, \beta, \alpha', \beta' = 1, 2, \ldots, f;\ \lambda \in D)$$

$$B = \sum_{\alpha=1}^{f}\sum_{\beta=1}^{f} De_{\alpha\beta}, \qquad \sum_{\alpha=1}^{f} e_{\alpha\alpha} = 1_B$$

can be transformed by a suitable inner automorphism of B in such a way that

$$\Lambda = \Lambda(f_1, f_2, \ldots, f_s; D, R)$$

$$= \Bigg\{ \sum_{i=1}^{f}\sum_{k=1}^{f} \lambda_{ik}e_{ik} \ \&\ \lambda_{ik} \in \Lambda(D, R)$$

$$\text{if } \sum_{j=1}^{h} f_h < i \leq \sum_{j=1}^{h+1} f_h, \quad \sum_{j=1}^{h} f_h < k \leq f$$

$$\&\ \lambda_{ik} \in J(\Lambda(D, R)) \text{ if } 1 \leq k \leq \sum_{j=1}^{h} f_h < i \Bigg\}$$

$(s > 0; f_i > 0\ (1 \leq i \leq s);$
$\sum_{i=1}^{s} f_i = f;\ h = 1, 2, \ldots, s;$
$J(\Lambda(D, R))$ the Jacobson radical of $\Lambda(D, R)$ which coincides with the only maximal ideal of $\Lambda(D, R))$ (Auslander–Goldman).

For the proof of the first part of Theorem 4 let us point out that every

maximal order of A is hereditary. Also, because of the absolute semisimplicity of A the discriminant ideal

$$\mathfrak{d}(\Lambda/R) = \text{ideal of } R \text{ generated by the determinants } \det(\mathrm{tr}(a_i b_k)) \text{ for all } 2n\text{-tuples } a_1, \ldots, a_n, b_1, \ldots, b_n \text{ of elements of } \Lambda \text{ and the reduced system trace function tr}$$

is not zero and that consequently for all prime ideals $\mathfrak{P}$ of R not dividing $\mathfrak{d}(\Lambda R)$ the $\mathfrak{P}$-localization $(\Lambda/(R-\mathfrak{P}))$ is a maximal order of A over $(R/(R-\mathfrak{P}))$. The discriminantal ideal $\mathfrak{d}(\Lambda R)$ is the power product of finitely many distinct prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ of R.

(H12) Λ is hereditary precisely if the finitely many localizations $(\Lambda/(R-\mathfrak{P}_i))$ are hereditary over $(R/(R-\mathfrak{P}_i))$ $(i = 1, 2, \ldots, t)$ where $\mathfrak{P}_1, \ldots, \mathfrak{P}_t$ run over the distinct prime ideal divisors of $\mathfrak{d}(\Lambda/R)$.

Form $J_{\mathfrak{d}(\Lambda/R)}(\Lambda) = \bigcap_{i=1}^{t} J_{\mathfrak{P}_i}(\Lambda)$, and its A-idealizer $\Lambda^{(1)}$. It follows that Λ is hereditary precisely if $\Lambda = \Lambda^{(1)}$. If Λ is not hereditary, then $\Lambda \subset \Lambda^{(1)}$. Setting $\Lambda^{(i+1)} = (\Lambda^{(i)})^{(1)}$ for $i = 1, 2, \ldots$ it follows that there is a nonnegative integer $h(\Lambda)$ such that $\Lambda^{(h(\Lambda))} = \Lambda^*$ is hereditary, and moreover,

$$\Lambda \subset \Lambda^{(1)} \subset \cdots \subset \Lambda^{(h(\Lambda))}.$$

It is clear that the formation of Λ^* is invariant under the automorphisms of A; $\Lambda^{**} = \sum \Lambda^* \cap (H_i E)$ is a crossed product of order A, $\Lambda^* \cap E$ is hereditary.

Thus the first part of Theorem 4 is established.

For the proof of the second part, use (H8). We may assume without loss of generality that A is simple.

Using (H6) and (H7) we may assume without loss of generality that the dedekind ring R is locally complete.

If φ is a finite unramified extension of the field F, then the integral closure of R in φ is a dedekind ring R_φ with φ as quotient field such that the Jacobson radicals are related by

$$J(R_\varphi) = J(R)R_\varphi .$$

For any R-order Ω the tensor product ring $\Omega \otimes_R R_\varphi$ is an R_φ-order with Jacobson radical

$$J\left(\Omega \underset{R}{\otimes} R_\varphi\right) = J(\Omega) \underset{R}{\otimes} R_\varphi .$$

In case Ω is hereditary then it follows from (H3) that $\Omega \otimes_R R_\varphi$ is hereditary, and conversely.

Applying a suitable unramified finite field extension to the ground field, it may be assumed without loss of generality that A is a ring of matrices of finite degree n over F, that the center of E is the algebraic sum of σ isomorphic fully ramified extensions of F, and that E itself is a ring of matrices of degree m over its center. It follows from the corollary of Theorem 3 and from (H11), that we may make the following additional assumptions without loss of generality:

$$E = \sum_{j=1}^{\sigma}{}^{\cdot} e_j E, \qquad 0 \neq e_j = e_j^2 \in \mathfrak{z}(E),$$

$$e_j e_{j'} = 0 \qquad (j \neq j';\ j, j' = 1, 2, \ldots, \sigma), \qquad \sum_{j=1}^{\sigma} e_j = 1_E,$$

$$e_j = \sum_{\alpha=1}^{m} e_{j\alpha\alpha} \qquad (1 \leq j \leq \sigma)$$

$$e_{j\alpha\beta} e_{k\alpha'\beta'} = \delta_{jk}\ \delta_{\beta\alpha'}\ e_{j\alpha\beta'}$$

$$(1 \leq j \leq \sigma,\quad 1 \leq k \leq \sigma;\quad \alpha, \beta, \alpha', \beta' = 1, 2, \ldots, m),$$

$$A = \sum_{h \in H_0}{}^{\cdot} \sum_{j=1}^{\sigma}{}^{\cdot} \sum_{\alpha=1}^{m}{}^{\cdot} \sum_{\beta=1}^{m}{}^{\cdot} h e_{j\alpha\beta} F,$$

$$\Lambda \cap E = \sum_{j=1}^{\sigma}{}^{\cdot} \sum_{\alpha=1}^{m}{}^{\cdot} \sum_{\beta=1}^{m}{}^{\cdot} J(R)^{\delta(\alpha,\beta)} e_{j\alpha\beta} F,$$

$$\delta(\alpha, \beta) = 0 \qquad \text{if} \quad m_{\mu-1} < \alpha < m_\mu,\ m_{\mu-1} < \beta \leq m,$$

$$0 = m_0 < m_1 < \cdots < m_s = m,$$

$$\delta(\alpha, \beta) = 1 \qquad \text{otherwise},$$

$$H = H_0 \square U(E), \qquad H_0 \text{ a finite group},$$

$$1 \to H_0 \xrightarrow{\varphi_0} \mathrm{Aut}(E) \text{ exact}, \qquad H_0\varphi_0 \cap \mathrm{Inn}(E) = 1_E,$$

$H_0\varphi_0$ acting transitively on $e_1, \ldots, e_\sigma$, the primitive idempotents of the center of E according to the operational rule

$$e_j(h\varphi_0) = e_{j(h\Delta)} \qquad (h \in H_0,\quad 1 \leq j \leq \sigma),$$

$$h^{-1} e_{j\alpha\beta} h = e_{j(h\Delta)\alpha\beta} \qquad (h \in H_0,\quad 1 \leq j \leq \sigma;\quad \alpha, \beta = 1, 2, \ldots, m),$$

$$\Lambda = \sum_{h \in H_0}{}^{\cdot} h J(R)^{v(h)} (\Lambda \cap E) \qquad (v(h) \in \mathbb{Z} \text{ for } h \text{ of } H_0),$$

$$v(h'h'') = v(h') + v(h'') \qquad (h', h'' \in H_0).$$

But since H_0 is finite and $\mathbb{Z}$ is torsion free, it follows that $v(h) = 0$ for all h

of H_0. Hence

$$\Lambda = \sum_{h \in H_0}{}' h(\Lambda \cap E).$$

There are elements h_i of H_0 satisfying

$$h_i^{-1} e_1 h_i = e_i \qquad (1 \leq i \leq \sigma),$$

so that the elements

$$e_{ik} = e_i h_i^{-1} e_1 h_k e_k \qquad (i, k = 1, 2, \ldots, \sigma)$$

satisfy the rules for matrix units

$$e_{ik} e_{i'k'} = \delta_{ki'} e_{ik'} \qquad (i, k, i', k' = 1, 2, \ldots, \sigma).$$

Furthermore,

$$e_{ii} = e_i \qquad (i = 1, 2, \ldots, \sigma).$$

Hence

$$\Lambda \cong ((\Lambda \cap e_1 H) \times H_{01} U(\Lambda \cap e_1 H))^{\sigma \times \sigma},$$

where

$$H_{01} = \{h \,|\, h \in H_0 \ \& \ e_1 h = h e_1\}$$

is the H_0-stabilizer of e_1 acting on the matrix units. We may assume without loss of generality that $\sigma = 1$ so that the order Λ is isomorphic to the tensor product ring over R of the hereditary order

$$\Lambda_1 = \sum_{\alpha=1}^{m} \sum_{\beta=1}^{m} J(R)^{\delta(\alpha, \beta)} e_{1\alpha\beta} \qquad \text{and} \qquad \Lambda_2 = \mathfrak{z}(E) \times H_0 .$$

We apply the

Lemma *The tensor product ring of a hereditary order Ω_1 over R with R as center and of any hereditary R-order Ω_2 with absolutely semisimple central quotient ring is a hereditary order.*

Proof Using (H8) and the invariance under finite unramified extension of the field of reference it suffices to consider the case that

$$F\Omega_1 = F^{m_1 \times m_1}, \qquad F\Omega_2 = (\mathfrak{z}E\Omega)^{m_2 \times m_2}.$$

Now the lemma follows from (H11) by explicit computation.

The application of the lemma reduces the proof of Theorem 4 to the case that E is a separable normal finite purely ramified extension of F, and that

$$H = H_0 \square U(E), \qquad H_0 \varphi_0 = \mathrm{Aut}(E/F), \qquad \Lambda = R_E \times H_0 , \qquad A \cong F^{n \times n}.$$

In this case the integral closure R_E of R in E is generated over R by an Eisenstein element ξ satisfying the equation

$$f(\xi) = \xi^n + \sum_{i=1}^{n} \lambda_i \pi \xi^{n-i} = 0 \qquad (J(R) = \pi R; \quad \lambda_i \in R \ (1 \leq i \leq n); \quad \lambda_n = 1).$$

where $f(t) = t^n + \sum_{i=1}^{n} \lambda_i \pi t^{n-i}$ is an irreducible monic polynomial of $R[t]$.

Choosing suitable matrix units of A we may assume that $A = F^{n\times n}$, $\Lambda \subseteq R^{n\times n}$ and that

$$\xi = \begin{bmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & 0 & 1 \\ -\pi & -\lambda_{n-1}\pi & \cdots & & -\lambda_1\pi \end{bmatrix}$$

is the accompanying matrix of f so that Λ is contained in the hereditary order $\tilde{\Lambda}$ of all matrices (α_{ik})

$$(\alpha_{ik} \in R, \quad \alpha_{ik} \in \pi R \quad \text{if } k < i \ (i, k = 1, 2, \ldots, n)).$$

Any maximal R-order of A containing Λ is of the form $X^{-1}R^{n\times n}X$ with nonsingular matrix X of $F^{n\times n}$ such that

$$\Lambda \in X^{-1}R^{n\times n}X, \qquad X\Lambda X^{-1} \subseteq R^{n\times n}.$$

But all irreducible R-representations of Λ are R-equivalent to the natural representation, so that there is also an element Y of $\mathrm{GL}(n, R)$ for which $Y^{-1}\Lambda Y = X\Lambda X^{-1}$. Hence

$$YX\Lambda(YX)^{-1} = \Lambda \qquad YX \in R\Lambda,$$

$$YX = \varepsilon\xi^{\nu} \qquad \text{with} \quad \nu \in \mathbb{Z}, \quad \varepsilon \in U(\Lambda), \qquad X = Y^{-1}\varepsilon\xi^{\nu},$$

$$X^{-1}R^{n\times n}X = \xi^{-\nu}\varepsilon^{-1}YR^{n\times n}Y^{-1}\varepsilon\xi^{\nu} = \xi^{-\nu}R^{n\times n}\xi^{\nu} \supseteq \xi^{-\nu}\tilde{\Lambda}\xi^{\nu}.$$

But by construction we have

$$\xi^{-1}\tilde{\Lambda}\xi = \tilde{\Lambda}$$

so that indeed

$$X^{-1}R^{n\times n}X \supseteq \tilde{\Lambda}.$$

Consequently, $\tilde{\Lambda}$ is contained in the intersection of all maximal orders containing Λ. On the otherhand, we know from Auslander–Goldman that every hereditary order is the intersection of the maximal orders to which it belongs. Therefore, the intersection of all maximal R-orders of A containing Λ is the hereditary order $\tilde{\Lambda}$. Thereby Theorem 4 is established.

Applications

I. Let G be a finite group containing a cyclic normal subgroup N that is its own centralizer in G and let Δ be a faithful irreducible rational integral representation of degree f.

It follows that the rational linear combinations of the matrices $g\Delta$ ($g \in G$) form a simple hypercomplex system $QG\Delta$ with $\mathbb{Z}$-order $\mathbb{Z}G\Delta$ that is the crossed product $\mathbb{Z}N\Delta \times GU(\mathbb{Z}N\Delta)$. Hence the intersection of all maximal $\mathbb{Z}$-orders of $\mathbb{Q}G\Delta$ containing $\mathbb{Z}G\Delta$ is a hereditary order $\overline{\mathbb{Z}G\Delta}$. The integral representation of G that are arithmetically equivalent to Δ fall in as many arithmetical equivalence classes as the irreducible integral representations of the hereditary order $\overline{\mathbb{Z}G\Delta}$ from which they are derived by restriction to G.

The locally integral representations of local hereditary orders can be determined explicitly.

The integral representations of global hereditary orders can be derived from its localizations and a generalization of a famous theorem of E. Steinitz.

II. Let A be a simple hypercomplex system over the rational number field $\mathfrak{Q}$. Let E a maximal commutative subfield of A that contains the center of A as subfield such that E is a normal extension of A.

Then A is a crossed product of E and $N_{U(A)}(E)$. There are corresponding crossed product $\mathbb{Z}$-orders.

The intersection of all maximal $\mathbb{Z}$-orders of A containing a crossed product order is a hereditary order.

Note that the crossed product orders fall into a finite number of equivalence classes under transformations by non zero elements of E.

6. Valuation Theoretic Interpretation

In pursuit of H. Benz's ideas we give here a *valuation theoretic interpretation* of Theorem 4. Given a dedekind ring R with quotient field F, we associate with every prime ideal $\mathfrak{p}$ of R a multiplicative valuation $\varphi = \varphi_{\mathfrak{p}}$

$$F \to \mathbb{R}^{\geq 0}\colon \varphi_{\mathfrak{p}}$$

characterized by the rules

$$x\varphi > 0 \Leftrightarrow x \neq 0 \qquad (x \in F), \tag{32a}$$

$$(xy)\varphi = (x\varphi)(y\varphi) \qquad (x, y \in F), \tag{32b}$$

$$(x + y)\varphi \leq \max(x\varphi, y\varphi) \qquad (x, y \in F), \tag{32c}$$

$$x\varphi \leq 1 \quad \text{if} \quad x \in R, \tag{32d}$$

$$x\varphi < 1 \quad \text{if} \quad x \in \mathfrak{p}. \tag{32e}$$

It follows that $\varphi_{\mathfrak{p}}$ is discrete such that

$$\max_{x \in \mathfrak{p}} x\varphi_{\mathfrak{p}} = \gamma_{\mathfrak{p}} = \gamma < 1. \tag{32f}$$

Given a semisimple hypercomplex system A over F we study the Kuerszak valuations

$$A \to \mathbb{R}^{\geq 0} : \Phi$$

of A which are characterized as those mappings Φ of A in $\mathbb{R} \geq 0$ for which

$$a\Phi > 0 \Leftrightarrow a \neq 0, \tag{33a}$$

$$(ab)\Phi \leq (a\Phi)(b\Phi) \qquad (a, b \in A), \tag{33b}$$

$$(a + b)\Phi \leq \max(a\Phi, b\Phi) \qquad (a, b \in A), \tag{33c}$$

and among them in particular the Kuerszak extensions of $\varphi_{\mathfrak{p}}$ characterized by the additional condition

$$F|\Phi = \varphi_{\mathfrak{p}}, \tag{33d}$$

as a consequence of which we have $\varphi_{\mathfrak{p}}$-multiplicativity

$$(xa)\Phi = (ax)\Phi = (a\Phi)(x\Phi) \qquad (a \in A, \quad x \in F). \tag{33e}$$

The trivial case $R = F$ usually is not considered. Furthermore, upon proceeding to the φ-completion, we may assume without loss of generality that R is local with $\mathfrak{p}$ as its only maximal ideal and complete discrete multiplicative valuation $\varphi = \varphi_{\mathfrak{p}}$. Denoting by

$$\mathfrak{M}(\Phi, \rho) = \{a \,|\, a \in A \;\&\; a\Phi \leq \rho\} \tag{33f}$$

the submodule of A formed by all elements of A for which the value of the Kuersak valuation Φ is not larger than ρ $(0 \leq \rho \in \mathbb{R})$ we find that the Kuersak valuation Φ of A is an extension of φ precisely if

$$\mathfrak{p}^{\nu}\mathfrak{M}(\Phi, \rho) = \mathfrak{M}(\Phi, \gamma^{\nu}\rho) \qquad (\nu \in \mathbb{Z}, \quad \rho \in \mathbb{R}^{\geq 0}). \tag{33g}$$

We note that the multiplicativity

$$\mathfrak{M}(\varphi, \rho_1)\mathfrak{M}(\varphi, \rho_2) = \mathfrak{M}(\varphi, \rho_1\rho_2) \qquad (\rho_1, \rho_2 \in \mathbb{R} \geq 0) \tag{33h}$$

is a consequence of (32b), whereas for Kuerszak valuations Φ of A in general only the weaker condition

$$\mathfrak{M}(\Phi, \rho_1)\mathfrak{M}(\Phi, \rho_2) \subseteq \mathfrak{M}(\Phi, \rho_1\rho_2) \qquad (\rho_1, \rho_2 \in \mathbb{R} \geq 0) \tag{33i}$$

holds that is tantamount to (33b). It implies that $\mathfrak{M}(\Phi, 1)$ is an R-order of A.

Definition The Kuerszak extension Φ of φ to a Kuerszak valuation Φ of A is said to be hereditary if it satisfies the conditions

$$\mathfrak{M}(\Phi, \rho_1)\mathfrak{M}(\Phi, \rho_2) = \mathfrak{M}(\Phi, \rho_1\rho_2) \qquad (\rho_1, \rho_2 \in \mathbb{R} \geq 0), \tag{33j}$$

$$\forall a\left(a \in A \;\&\; a \bigcap_{\rho<1} \mathfrak{M}(\Phi, \rho) \subseteq \bigcap_{\rho<1} \mathfrak{M}(\Phi, \rho) \Rightarrow a\Phi \leq 1\right). \tag{33k}$$

As a consequence of these conditions and of (H3) the R-order $\Lambda = \mathfrak{M}(\Phi, 1)$ of A is hereditary such that

$$J(\Lambda)^{e_\Phi} = \mathfrak{p}\Lambda \qquad (e_\Phi \in \mathbb{Z} > 0), \tag{33l}$$

$$a\Phi = \gamma^{\nu/e_\Phi} \qquad \text{if} \quad a \in J(\Lambda)^\nu; \quad a \notin J(\Lambda)^{\nu+1} \quad (0 \neq a \in A) \tag{33m}$$

and conversely (33l) implies that (33m) defines a hereditary Kuerszak extension Φ of φ.

Here the number e_Φ is called *ramification index* of Φ over φ because the Φ-values $\neq 0$ form the cyclic group generated by γ^{1/e_Φ} which contains the value group of φ as a subgroup of index e_Φ.

Theorem 4 admits the following valuation theoretic interpretation:

Let A a simple ring of finite dimension over its center F with complete discrete multiplicative valuation φ such that A is crossed product of some semisimple subalgebra E.

Then there is a hereditary Kuerszak extension Φ_E of φ that is unique up to inner automorphism of E.

For given Φ_E there is a Kuerszak extension Φ_A of (Kuerszak extension of Φ_E) which is unique up to inner transformation by the units of the center of E.

REFERENCES

[1] H. Benz, Untersuchungen zur Arithmetik in lokalen einfachen Algebren, inbesondere über maximalen Teilkörpern, I, *Crelle* **225** (1967), 30–75.

[2] O. Taussky, Additive commutators between 2 × 2 matrix representations of orders in identical or different quadratic number fields, *Amer. Math. Soc.* **80** (1974), 885–887.

[3] O. Taussky, A result concerning classes of matrices, *J. Number Theory* **6** (1974), 64–71.

[4] O. Taussky, Additive commutators of rational 2 × 2 matrices, *Linear Algebra and Appl.* **12** (1975), 1–6.

A
B 7
C 8
D 9
E 0
F 1
G 2
H 3
I 4
J 5

Number Theory and Algebra

ZASSENHAUS

512.
7
NUM

ACADEMIC PRESS

ISBN 0-12-776350-3